Secure Secret Sharing Schemes for Reconstruction of Digital Images: A Survey

Arvind Singh Choudhary, Dr.Manoj Kumar

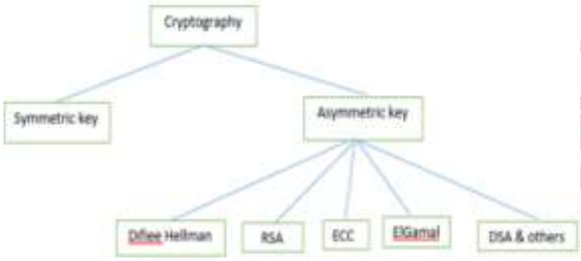
Department of Computer Science Engineering, Government Engineering College Bharatpur, Rajasthan, India
Department of Computer engineering & application, GLA University Mathura (UP)

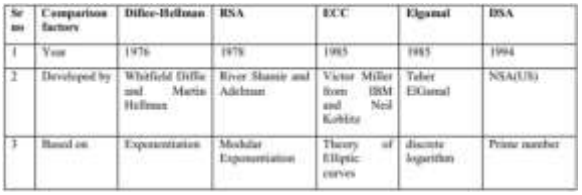
Abstract:- In many situations, the technique to hide a secret is needed. One might need to hide a password, an encryption Key, a secret recipe, and etc. Information can be secured with encryption, but the need to secure the secret key used for such encryption is important too. Consider, we encrypt our important files with one secret key and if that secret key is lost then all the important files will be inaccessible. Thus, secure and efficient key management mechanisms are required. One of them is secret sharing scheme (SSS) that allows to split the secret into several shares which will get distributed to all the participants. The secret can be recovered once these parties collaborate in some way. This survey paper will study these schemes and explain the need for the secret sharing and their security. Across the years, various schemes have been presented. This paper will review some of them varying from trivial schemes to threshold based ones.

Keywords - Secret splitting, Shamir's Secret Sharing Scheme, Threshold Schemes,Visual Cryptography

I. Introduction

Nowadays transmitting multimedia data by means of all-pervasive Internet is the trend gaining interest [34]. With the advent of e-commerce, it has become extremely essential to tackle the sensitive issues of affording data security, especially in the ever-blooming open network environment of the modern era. The encrypting technologies of the time-honored cryptography are generally employed to shelter data safety extensively. Cryptography is used to send and receive encrypted information which can be decrypted only by the sender or receiver. This technique is mainly used to store and transmit the data in an appropriate manner that can be read and processed only by the intended person. In the cryptography process,





Sr no	Comparison factors	Diffie-Hellman	RSA	ECC	Elgamal	DSA
1	Year	1976	1978	1985	1985	1994
2	Developed by	Whitfield Diffie and Martin Hellman	River Shamir and Adelman	Victor Miller from IBM and Neil Koblitz	Taher ElGamal	NSA(US)
3	Based on	Exponentiation	Modular Exponentiation	Theory of Elliptic curves	discrete logarithm	Prime number

Table 1: Comparison table of Asymmetric Algorithms

A secret image kept in a single information-carrier could be easily retrieved or damaged by unauthorized entity. Once the confidential image information is illegitimately retrieved, the unauthorized person makes use of the content for their own benefits. In the gigantic internet communication, the secret image sharing schemes can be used to share a secret image with utmost confidentiality over unsecured public channels. In this scheme a secret image is programmed into n shadows of arbitrary prototypes. It is possible to decode the secret image visually by superimposing a qualified subset of shadows. Nevertheless, no secret image can be acquired from the superposition of an illegal subset. This paper describes detailed overview of the current trends and previous contributions of the research on digital image security. The limitation of the each paper was studied well to focus better on the future directions on secret image sharing schemes.

Image secret sharing (ISS) has seen an immense growth in modern day world due to excess internet usability along with growing insecurity due to advanced attacks from the hackers. Secret sharing methods play a very important part in visual cryptography(VC) which began with introduction of "(k, n) threshold" scheme introduced by Shamir and Blakeley in 1979. In this scheme a secret is divided/encoded into 'n' shares or meaningless noisy images. The message to be hidden can only be constructed by stacking (combining with some logic) up at least 'k' number of shares/transparencies. Various advancements have happened in ISS with introduction of the "(k, n) threshold" based scheme to images. It has led to development of new schemes like probability based ISS, extended ISS, ISS using Cloud, and progressive ISS with perfect reconstruction capability or perfect data retrieval capability etc. These techniques are judged using the parameters like security robustness, pixel expansion and contrast of retrieved image.

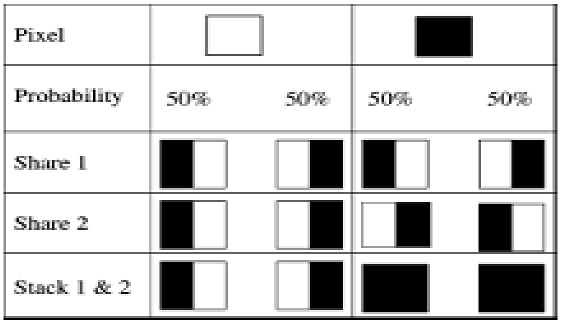
The ISS schemes can be made more robust and secure by integrating various features like introducing progressive ISS feature with Cloud and further increasing data payload by increasing ability to embed more data without decreasing the security and quality of retrieved original secret data.

In this paper different ISS schemes have been surveyed and compared taking into consideration security, pixel expansion and contrast loss along with future scope of these techniques and application areas have also been discussed to get the scope of future research in the area.

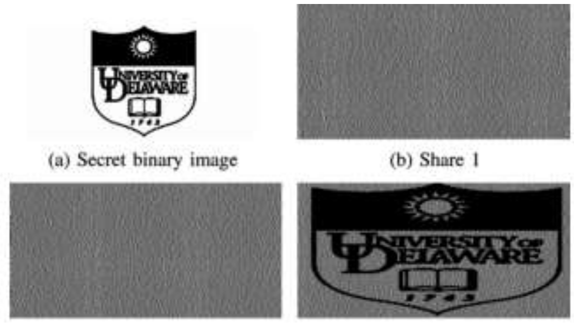
A secret-sharing scheme is a method by which a dealer distributes shares to parties such that only authorized subsets of parties can reconstruct the secret. Secret-sharing schemes are important tools in cryptography and they are used as a building box in many secure protocols, e.g., general protocol for multiparty computation, Byzantine agreement, threshold cryptography, access control, attribute-based encryption, and generalized oblivious transfer. In this survey, we will describe the most important constructions of secret-sharing schemes, explaining the connections between secret-sharing schemes and monotone formulae and monotone span programs. The main problem with known secret-sharing schemes is the large share size: it is exponential in the number of parties. We conjecture that this is unavoidable. We will discuss the known lower bounds on the share size. These lower bounds are fairly weak and there is a big gap between the lower and upper bounds. For linear secret-sharing schemes, which is a class of schemes based on linear algebra that contains most known schemes, super-polynomial lower bounds on the share size are known. We will describe the proofs of these lower bounds. We will also present two results connecting secret-sharing schemes for a Hamiltonian access structure to the NP vs. coNP problem and to a major open problem in cryptography – constructing oblivious-transfer protocols from one-way functions.

Encryption is the conversion of plaintext (ordinary text or clear text) into cipher text and the reverse process is called decryption and the people who are working in this domain are called as cryptographers[19]. With the emergence of multimedia applications, there is a huge demand for transmission and secured storage of information. So security is indispensable for proper data protection. If the information is protected, the intruders may not be able to distort the data. It becomes challenging to transmit the data in a secured and proper manner. Cryptographic techniques afford the confidentiality and security by reducing the prospect of adversaries. Unlike traditional cryptographic methods such as Data Encryption Standard (DES) scheme and Advanced Encryption Standard (AES) scheme, the Visual Cryptography (VC) scheme provides fast decryption without any complex computation.

Visual Cryptography (secret sharing scheme) is a modern cryptographic technique used to share the secret data in a secure pattern, maintained with utmost confidentiality. A sender transmits the secret data which is divided into shadows and it holds hidden information. When all of these shadows are aligned and stacked together, it tends to expose the secret data information to the receiver [12]. The main role of VC scheme is to encrypt the secret data with the help of partitioning process. The private message cannot be revealed by the help of some split data‟s. The original image requires all split data‟s to be revealed. The process of visual cryptography is to divide an image into prearranged number of parts and then without any computation or algorithm, the secret data can be revealed by aligning and stacking together. Another, secret sharing scheme is Visual Secret Sharing (VSS), based on the (k-n) threshold concept. This method works out of n shadow with any k or more reconstructed shadows to retrieve the original secret by superimposing the shadows that eliminates complex computations.



Pixel	□		■	
Probability	50%	50%	50%	50%
Share 1	■□	□■	■□	□■
Share 2	■□	□■	□■	■□
Stack 1 & 2	■□	□■	■■	■■



(a) Secret binary image

(b) Share 1

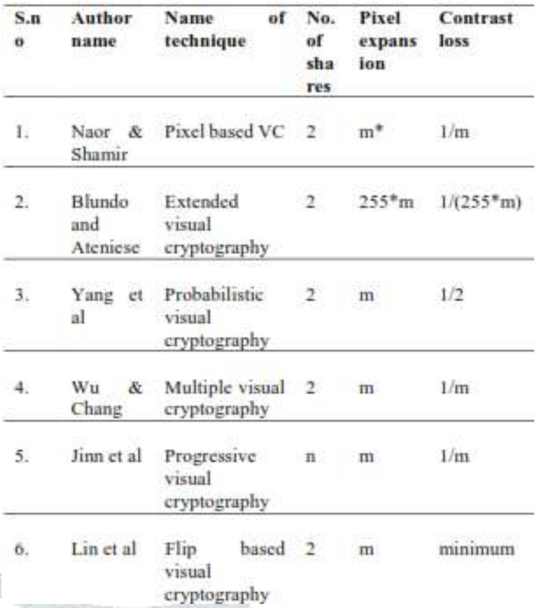
Figure – 2-out-of 2 Visual Cryptography

The Secret Sharing Schemes (SSS) is one of the key management or establishment schemes invented separately in 1979 by both Shamir [1] and Blakey [8] as a solution to safeguard cryptographic keys. Secret sharing schemes are also used to protect other types of secrets, such as a secret recipe or a password to a bank vault, control access of nuclear weapons and others. We need these schemes because many cryptosystems that use a single master key have various vulnerabilities. For instance, if the master key is disclosed to the public by accident or by an attacker, this will compromise the entire system. Also, if the master key is lost, then all the other keys it protects become inaccessible. Additionally, if the owner of the master key turns out to be disloyal then all sensitive information will be leaked to the opponents. In addition, these schemes are useful when we don’t want to save the secret in a single place or when we don’t trust a single person owning a certain secret. From these reasons comes the need for SSS. To see how SSS works in real life scenario consider a country that for various reasons does not want the access control of its nuclear weapon to be activated by a single person only[4]. Thus they can involve for example three participants, the President, Defense Minister and the Defense Ministry, where any two out of these three can gain control of the nuclear weapon.

Various ISS schemes have received a lot of attention with the increase in internet connectivity and data processing. It has developed an upper hand over the traditional cryptography and data embedding schemes. In visual secret sharing, an image or an image containing secret is converted/encrypted into number of shares and then the transmissions happens over any communication channel or a network. Data can be embedded into the images through various secure algorithms like hiding in encrypted images as described in [33]. Hiding data is very important for various applications like hiding in medical images [15], hiding images for covert communication [3] etc. The original image or the secret is shared after converting it into number of transparencies/shadows which depends upon the level of security needed. After these shares are transmitted through any network, the secret at the receiver is constructed back by stacking up the shares without any complex cryptographic algorithm. These multiple shadow images individually do not provide the idea of the secret which shows that the basic requirement of the image security is enhanced during the process of image secret sharing.

Initially the idea of secret sharing was introduced by Blakeley [1] and Shamir [2]. This concept was extended to images giving birth to cryptography based VSS that was first proposed by "Naor and Shamir" [3]. The "(k, n) threshold" (where k acts as threshold) based image secret sharing put forward by "Noar and Shamir" segregates the secret image (which contains the secret) into "n" number of meaningless shares. The secret image or image containing the secret data is recovered by stacking up/combining at least "k" shares or more together and stacking up/combining less than "k" shares do not give access to any of the secret information. Logical 'OR' or 'XOR' is used to reconstruct the image from the shares. This has been illustrated in the Fig.1. As the image is divided/encoded into a number shares, this gives rise to various issues. The most common problem that is encountered by piling up of shares is the pixel expansion. The limitation of pixel expansion [24]

Results into the requirement of more memory and more bandwidth. The oldest form of visual cryptography techniques had also various other drawbacks like need for codebook, low quality of constructed image and alignment of pixels. It was till 1997, binary and greyscale images had been encoded through visual cryptography. First VSS scheme that was used to encode color images was introduced by Verhaul and Tilburg [4]. The shares developed in this scheme were meaningless. Various other ISS schemes were developed after a vast research to overcome various drawbacks of old visual cryptographic schemes. Some of these schemes were used in binary images e.g. progressive ISS, natural ISS, extended ISS etc., while some were developed for greyscale and RGB images e.g. ISS using halftone, ISS using image hatching, chaos based ISS etc. Most researched and implemented schemes are I SS using random grids, extended visual cryptography, flip based visual cryptography, multiple image cryptography, probability based ISS, ISS based on circular shares, progressive ISS, ISS based on cloud etc. These schemes were researched more to decrease pixel expansion, increase security, increase contrast of constructed images and improving alignment of shares. In this review paper, we will discuss/survey the preferred ISS techniques, their advantages, drawbacks and application areas. Various parameters that are used for the comparison of a scheme with other are PSNR, NPCR [25], UACI [25] and pixel expansion ratio.



S.no	Author name	Name of technique	No. of shares	Pixel expansion	Contrast loss
1.	Naor & Shamir	Pixel based VC	2	m*	1/m
2.	Blundo and Ateniese	Extended visual cryptography	2	255*m	1/(255*m)
3.	Yang et al	Probabilistic visual cryptography	2	m	1/2
4.	Wu & Chang	Multiple visual cryptography	2	m	1/m
5.	Jinn et al	Progressive visual cryptography	n	m	1/m
6.	Lin et al	Flip based visual cryptography	2	m	minimum

Table-Comparison between Cryptographic Techniques

Nowadays transmitting multimedia data by means of all-pervasive Internet is the trend gaining interest [34]. With the advent of e-commerce, it has become extremely essential to tackle the sensitive issues of affording data security, especially in the ever-blooming open network environment of the modern era[3]. The encrypting technologies of the time-honored cryptography are generally employed to shelter data safety extensively. Cryptography is used to send and receive encrypted information which can be decrypted only by the sender or receiver. This technique is mainly used to store and transmit the data in an appropriate manner that can be read and processed only by the intended person. In the cryptography process,

Encryption is the conversion of plaintext (ordinary text or clear text) into cipher text and the reverse process is called decryption and the people who are working in this domain are called as cryptographers[4]. With the emergence of multimedia applications, there is a huge demand for transmission and secured storage of information. So security is indispensable for proper data protection. If the information is protected, the intruders may not be able to distort the data. It becomes challenging to transmit the data in a secured and proper manner. Cryptographic techniques afford the confidentiality and security by reducing the prospect of adversaries. Unlike traditional cryptographic methods such as Data Encryption Standard (DES) scheme and Advanced Encryption Standard (AES) scheme, the Visual Cryptography (VC) scheme provides fast decryption without any complex computation. Visual Cryptography (secret sharing scheme) is a modern cryptographic technique used to share the secret data in a secure pattern, maintained with utmost confidentiality[5]. A sender transmits the secret data which is divided into shadows and it holds hidden information. When all of these shadows are aligned and stacked together, it tends to expose the secret data information to the receiver [22]. The main role of VC scheme is to encrypt the secret data with the help of partitioning process. The private message cannot be revealed by the help of some split data‟s. The original image requires all split data‟s to be revealed. The process of visual cryptography is to divide an image into prearranged number of parts and then without any computation or algorithm, the secret data can be revealed by aligning and stacking together. Another, secret sharing scheme is Visual Secret Sharing (VSS), based on the (k-n) threshold concept. This method works out of n shadow with any k or more reconstructed shadows to retrieve the original secret by superimposing the shadows that eliminates complex computations.

II. Literature Survey

In visual cryptography (VC) for grayscale image, size reduction leads to bad perceptual qualityto the reconstructed secret image. To improve the quality, the current efforts are limited to the design of VC algorithm for binary image, and measuring the quality with metrics that are not directly related to how the human visual system perceives halftone images. We propose an analysis-by-synthesis (AbS) framework [1] to integrate the

Half toning process and the encoding: the secret pixel/block is reconstructed from the shares in the encoder and the error between the reconstructed secret and the original secret images is fed back and compensated concurrently by the error diffusion process.

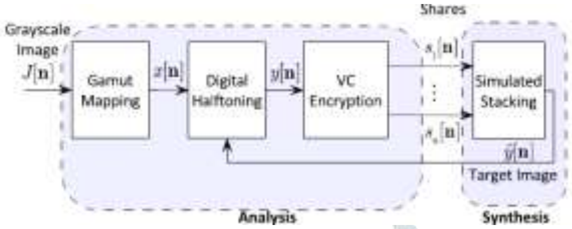


Fig. The block diagram of the Proposed Framework

In doing so, the error between the reconstructed secret and original secret is pushed to high frequency band, thus producing visually pleasing reconstructed secret image. This framework is simple and flexible in that it can be combined with many existing size-invariant VC algorithms, including probabilistic VC, random grid VC, and vector/block VC. More importantly, it is proved that this AbS framework is as secure as the traditional VC algorithms. Experimental results demonstrate the effectiveness of the proposed AbS framework.

A d-multiplicative secret sharing (d-MSS) scheme allows the players to multiply d shared secrets without recovering the secrets by converting their shares locally into an additive sharing of the product [2].

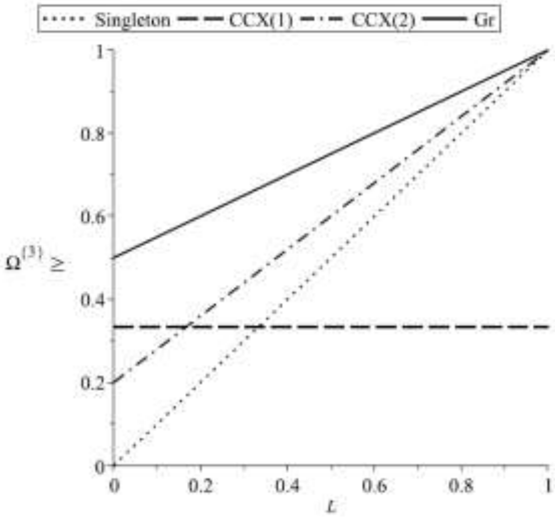


Fig: - Comparison on Asymptotic Bounds on the threshold gap for q=2

It has been proved that the d-MSS among n players is possible if and only if no d unauthorized sets of players cover the whole set of players (type Qd). Although this result implies some limitations on SS in the context of MPC, the d-multiplicative property is still useful for simplifying complex tasks of MPC by computing the product of d field elements directly and non-interactively without any setup. This paper aims to improve the usefulness of the d-MSS by enhancing the security against malicious adversaries. First, we introduce the notion of verifiably multiplicative SS, verifiably MSS for short, which is mainly formalized for detecting malicious behaviors. Informally, an SS scheme is verifiably d-multiplicative if the scheme is d-multiplicative and further enables the players to locally generate a share of a proof that the summed value is correct (i.e., the product of d shared secrets). Secondly, we prove that there is no error-free verifiably MSS scheme whose decoder of the proof is additive, and that by accepting an error probability that can be chosen arbitrarily, there exists a verifiably d-MSS scheme realizing a given access structure if and only if the access structure is of type Qd. In the proposed construction, each share of a proof consists of only two field elements. This result means that we can efficiently achieve the optimal resiliency of the standard d-MSS even against malicious adversaries. We note that by allowing a general class of decoders that includes a linear one, there is an error-free verifiably d-MSS scheme if the access structure is of type Qd+1. Finally, we generalize the dmultiplicative property to a d-or-less version where the number d of multiplied secrets with d≤ d is not known in advance. We show that a d-or-less MSS scheme can be constructed from any d-MSS scheme of the same access structure with a constant overhead, and the feasibility of (verifiably) d-MSS implies that of (verifiably) d-or-less MSS.

In this paper, we consider linear secret sharing schemes over a finite field Fq, where the secret is a vector in F q and each of the n shares is a single element of Fq [3]. We obtain lower bounds on the so-called threshold gap g of such schemes, defined as the quantity r−t where r is the smallest number such that any subset of r shares uniquely determines the secret and t is the largest number such that any subset of t shares provides no information about the secret. Our main result establishes a family of bounds which are tighter than previously known bounds for ≥2. Furthermore, we also provide bounds, in terms of n and q, on the partial reconstruction and privacy thresholds, a more finegrained notion that considers the amount of information about the secret that can be contained in a set of shares of a given size. Finally, we compare our lower bounds with known upper bounds in the asymptotic setting.

Reversible data hiding in encrypted images (RDHEI) has been introduced for preserving image privacy and data embedding. RDHEI usually involves three parties; namely, the image provider, data hider, and receiver [4]. On the security with key setting, there are three categories: share independent secret keys (SIK), shared one key (SOK) and share no secret keys (SNK). In SIK, the image provider and data hider must respectively and independently share secret keys with the receiver,

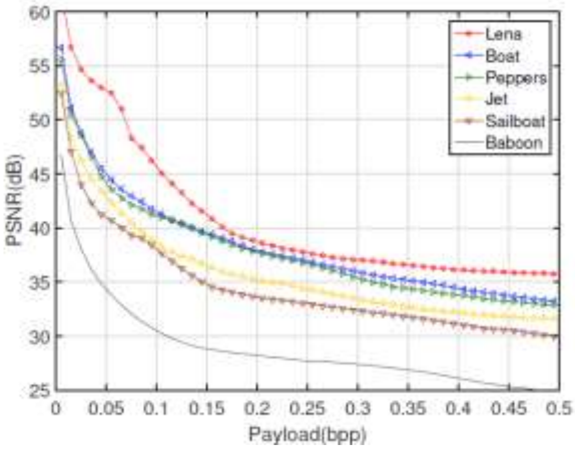


Fig. .- PSNR and Payload of a proposed SOK type Method

whereas in SNK, no secret key is shared. However, the literature works proposed SNK-type schemes by using homomorphic encryption (with exorbitant computation cost). In this paper, we address shared one key (SOK) setting, where only the image provider shares a secret key with the receiver, and the data hider can embed a secret message without any knowledge of this key. To realize our SOK scheme in a simple manner, we propose a new technique by using multi-secret sharing as the underlying encryption, which indeed induces a blow-up issue of the key size. For preserving the efficiency of the key size, we apply a compression by using lightweight cryptographic algorithms. Then, we demonstrate our SOK scheme based on the proposed techniques, and show effectiveness, efficiency, and security by experiments and analysis.

User authentication is one of the most fundamental security problems that design effective ways of identifying single or multiple entities using shared information, signatures, or intrinsic properties of the user(s). Password-based authentication is standard in the computer systems; however, passwords usually have low entropy content, and therefore vulnerable to dictionary attacks. Furthermore, password storage and simultaneous multiparty authentication also pose security and privacy concerns. Secret sharing-based techniques during password enrollment are found to be helpful in securing key storage in the authentication server [5], and in assisting multiparty authentication without exposing individual identity. However, secret sharing techniques, such as Shamir's secret sharing, are computationally expensive; therefore, its implementation in power-constrained systems is elusive. To address these problems, we have demonstrated how secure and lightweight user authentication techniques can be designed using several wellknown properties of memristive devices. For developing our secret sharing-based computationally lightweight user authentication protocols, first, we define essential utility functions, such as Read State, SET Pulse Count, Preconditioning, and so on, for controlling conductive filament formation in memristive devices. Next, we demonstrate the implementation of hardware-dependent simple authentication protocols that can ensure secure key storage usingsecretsharingprotocol derived from ShamirandNaor's visual cryptographic constructs. Then, we lay out the required hardware design and discuss the potential attacks to these protocols and the corresponding countermeasures. We conclude that, under realistic attacking assumptions, the proposed protocols are secure. Finally, using PTM's 65-nm MOSFET models and Stanford's variation-aware memristor models, we perform HSPICE simulation of the secret-reconstruction and authentication units to demonstrate the reliability of the hardware designs against SET–RESET unbalance, noise, temperature fluctuations, and aging.

The well-known Thien and Lin's (k, n) secret image sharing (SIS) scheme and its extended versions are threshold schemes [6], in which a secret image is shared among n shadow images and it can be recovered from any k shadow images. To reduce the size of shadow image, in those schemes, secret image pixels are embedded in all coefficients of (k□1)-degree polynomial to generate the shadows. Also, the secret pixels are permuted before the sharing to address the residual-image problem on shadow images. Due to the above two approaches, partial secret information can be exposed from (k□1) shadow images, and thus the threshold properties of those schemes will be compromised. To overcome this weakness, we propose a novel (k, n)-SIS scheme based on encrypted pixels, whose shadow image size is slightly larger than that of Thien and Lin's scheme. By slightly modifying the secret image, we also propose a modified (k, n)-SIS scheme with the same shadow size of Thien and Lin's scheme.

R7

This paper considers a distributed storage system, where multiple storage nodes can be reconstructed simultaneously at a centralized location. This centralized multi-node repair (CMR) model is a generalization of regenerating codes that allow for bandwidth efficient repair of a single failed node. This work focuses on the trade-off between the amount of data stored and repair bandwidth in the CMR model. In particular, repair bandwidth bounds are derived for the minimum storage multi-node repair (MSMR) and the minimum bandwidth multinode repair (MBMR) operating points. The tightness of these bounds is analyzed via code constructions. The MSMR point is characterized by codes achieving this point under functional repair for the general set of CMR parameters, as well as with codes enabling exact repair for certain CMR parameters. The MBMR point, on the other hand, is characterized with exact repair codes for all CMR parameters for systems that satisfy a certain entropy accumulation property. Finally, the model proposed here is utilized for the secret sharing problem, where the codes for the multi-node repair problem are used to construct communication efficient secret sharing scheme with the property of bandwidth efficient share repair

R8

Traditional approaches to secret key establishment based on common randomness have been based on certain restrictive assumptions, such as considering the available common randomness to consist of independent and identically distributed (i.i.d) repetitions of correlated random variables. Unfortunately, the i.i.d assumption does not generally reflect the conditions of real-life scenarios. For this reason, the current paper investigates the key-establishment potential of a more pragmatic model, in which all parties have access to imperfect information about a common source modeled as a Markov chain. Each party's information thus comes in the form of a hidden Markov model (HMM)and, since the different parties share the same underlying Markov chain, we call the overall model a Sibling Hidden Markov Model (SHMM). The paper studies upper and lower bounds on the secret key capacity for various types of SHMM. The difficulty of the problem emerges from its prohibitive computational cost. To address this obstacle, we represent the joint probability of the observations as the L1 norm of a Markov random matrix, and use its convergence to a Lyapunov exponent.

R9

An important problem in secret sharing schemes is minimizing the share size. For (k,n)-threshold schemes and (k,L,n)-ramp schemes, constructions that minimize the share size are known. This paper presents optimal constructions for a more general class of access structures in which subsets with the same cardinality have the same amount of information about the secret. We refer to schemes with such uniform access structures as uniform secret sharing. We first derive a tight lower bound for share entropy and then present an optimal construction. Our lower bound exceeds that previously reported. The optimal construction encodes the secret value using one or more ramp schemes.

R10

Quick Response (QR) codes have been widely used in applications such as data storage and high-speed machine reading. Anyone can gain access to the information stored in QR codes; therefore, they are unsuitable for encoding secret information without the addition of cryptography or other protection. In this paper, we propose a visual secret sharing scheme to encode a secret QR code into several shares. In contrast with other techniques, the shares in our scheme are valid QR codes that can be decoded with some specific meaning by a standard QR code reader, thereby avoiding raising suspicion in potential attackers. Moreover, the secret message is recovered by XOR-ing the qualified shares, an operation that can easily be performed using smartphones or other QR scanning devices. Experimental results show that the proposed scheme is both feasible and reasonably secure. Our scheme's high sharing efficiency is also highlighted in this paper.

R11

Secret sharing schemes with optimal and universal communication overheads have been obtained independently by Bitar et al. and Huang et al. However, their constructions require a finite field of size q > n, where n is the number of shares, and do not provide strong security. In this work, we give a general framework to construct communication efficient secret sharing schemes based on sequences of nested linear codes, which allows touseinparticularalgebraicgeometrycodesandallowstoobtain strongly secure and communication efficient schemes. Using this framework, we obtain: 1) schemes with universal and close to optimal communication overheads for arbitrarily large lengths n and a fixed finite field, 2) the first construction of schemes with universal and optimal communication overheads and optimal strong security (for restricted lengths), having in particular the component-wise security advantages of perfect schemes and the security and storage efficiency of ramp schemes, and 3) schemes with universal and close to optimal communication overheads and close to optimal strong security defined for arbitrarily large lengths n and a fixed finite field.

R12

The classical threshold secret sharing scheme by Shamir requires high computation complexity. Many fast secret sharing schemes have been proposed to reduce the computation cost. Another problem of perfect secret sharing scheme is the large share size. Ramp sharing schemes were proposed as a solution to reduce the share size with sacrificing secrecy to some extent. This work proposes a new ramp scheme, which is adapted from the zigzag-decodable erasure codes for data storage systems. The scheme is shown to approach a linear ramp scheme when the secret size grows to infinity. It is conceptually easy to understand, and has low computation cost, since both its encoding and decoding algorithms are based only on the XOR and bitwise-shift operations.

R13

The aim ofthispaperisto maximize therange of the access control of visual secret sharing (VSS) schemes encrypting multiple images. First, the formulation of access structures for a single secret is generalized to that for multiple secrets. This generalization is maximal in the sense that the generalized formulation makes no restrictionson access structures;in particular, it includes the existing ones as special cases. Next, a sufficient condition to be satisfied by the encryption of VSS schemes realizing an access structure for multiple secrets of the most general form isintroduced,and two constructionsof VSS schemes with encryption satisfying this condition are provided. Each of the two constructions has its advantage against the other; one is more general and can generate VSS schemes with strictly better contrast and pixel expansion than the other, while the other has a straightforward implementation. Moreover, for threshold access structures, the pixel expansions of VSS schemes generated by the latter construction are estimated and turn out to be the same as those of the existing schemes called the threshold multiplesecret visual cryptographic schemes. Finally, the optimality of the former construction is examined, giving that there exist access structures for which it generates no optimal VSS schemesThe aim ofthispaperisto maximize therange of the access control of visual secret sharing (VSS) schemes encrypting multiple images. First, the formulation of access structures for a single secret is generalized to that for multiple secrets. This generalization is maximal in the sense that the generalized formulation makes no restrictionson access structures;in particular, it includes the existing ones as special cases. Next, a sufficient condition to be satisfied by the encryption of VSS schemes realizing an access structure for multiple secrets of the most general form isintroduced,and two constructionsof VSS schemes with encryption satisfying this condition are provided. Each of the two constructions has its advantage against the other; one is more general and can generate VSS schemes with strictly better contrast and pixel expansion than the other, while the other has a straightforward implementation. Moreover, for threshold access structures, the pixel expansions of VSS schemes generated by the latter construction are estimated and turn out to be the same as those of the existing schemes called the threshold multiplesecret visual cryptographic schemes. Finally, the optimality of the former construction is examined, giving that there exist access structures for which it generates no optimal VSS schemes

R14

Recently, multiple (k, n) region-incrementing VCSs (RIVCSs) have been proposed that can gradually reconstruct secrets in a single image. In (k, n)-RIVCS, the secret image is subdivided into multiple regions in such a way that any t shadow images, where k □ t □ n, can be used to reveal the secret in the (t−k+1)-th region. This region-incrementing property provides progressive decoding. However, the regions in previous RIVCSs are disjointed: no two regions have overlapping areas. In this paper, we discuss a (k, n) region-in-region progressive VCS (RPVCS). Our (k, n)-RPVCS has (n□k+1) secrecy-level regions, and each region can be located within any previous region. This new type of region allocation not only provides more areas in which to hide the secret compared to the nonoverlapping regions in RIVCS but also provides different presentation methods in progressive decoding.

R15

Shamir's secret sharing is used as an important underlying primitive in many other cryptographic schemes, such as group authentication and group key agreement schemes. Although Shamir secret sharing has unconditional security, it is not necessarily the case for the protocols founded on that. A common imperfect assumption in such schemes is to be satisfied of only hiding the polynomials coefficients from the adversary. In this direction, we present a new method that can be potentially used for cryptanalysis of some Shamir's secret sharing-based schemes. This method is called the linear subspace cryptanalysis, in which the attack problem is made equivalent to the problem of studying the belongingness of a vector to a given linear subspace. Using the proposed method, we analyse the Harn's group authentication protocol, which is a remarkable scheme recently designed based on Shamir's scheme. This scheme has two main variants: one-time asynchronous and multiple-time asynchronous. In the one-time variant, it has been evaluated by the designer that the number of group members should be bounded to $n <kt + 1$, in order to make the scheme resistant against outside attacks. This constraint has been relaxed in the multiple-time variant, backed by the hardness of discrete logarithm problem. In this paper we show that neither confining the number of group members nor using discrete logarithm have made the one-time and multiple-time variants of this scheme resistant against impersonation attack. We show that in both cases, an outside attacker can impersonate an authorized group member in a polynomial time, when at least $t + k−1$ authorized members are participating in the group authentication session. The main observation, based on which the attack works, is that the dimension of the linear subspace spanned by the Lagrange components for any predefined set of users never exceeds $t+k−1$

R16

This paper first introduces a (k,n)-sharing matrix S(k,n) and its generation algorithm. Mathematical analysis is provided to show its potential for secret image sharing. Combining sharing matrix with image encryption, we further propose a lossless (k,n)-secret image sharing scheme (SMIE-SIS). The chaotic image encryption is extremely sensitive to ciphertext. Little change in the ciphertext will lead to failure of noise-like decrypted results even with right key. Thus, even though sharing matrix will recover part of ciphertext information when less than k secretsharesarecombined,itsmissinginformationwillresultin a wrong key and a noise-like decryption result, keeping the secret from leakage. Only with no less than k shares, all the ciphertext information and security key can be reconstructed, which results in a lossless recovery of original information.

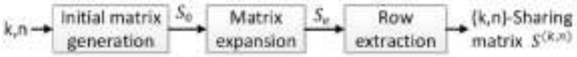


Fig. The Proposed (k,n) Sharing Matrix Generation Algorthm

This can be proved by the correctness and security analysis. Performance evaluation and security analysis demonstrate that the proposed SMIE-SIS with arbitrary settings of k and n has at least five advantages: (1) It is able to fully recover the original image without any distortion. (2) It has much lower pixel expansion than many existing methods. (3) Its computation cost is much lower than the polynomial-based secret image sharing method. (4) It is able to verify and detect a fake share. (5) Even using the same original image with the same initial settings of parameters, every execution of SMIE-SIS is able to generate completely different secret shares that are unpredictable and non-repetitive. This property offers SMIE-SIS a high level of security to withstand many different attacks.

R17

Access control ensures that only the authorized users of a system are allowed to access certain resources or tasks. Usually, according to their roles and responsibilities, users are organized in hierarchies formed by a certain number of disjoint classes. Such hierarchies are implemented by assigning a key to each class, so that the keys for descendant classes can be efficiently derived from classes higher in the hierarchy. However, pure hierarchical access may represent a limitation in many real-world cases. In fact, sometimes it is necessary to ensure access to a resource or task by considering both its directly responsible user and a group of users possessing certain credentials. In this paper, we first propose a novel model that generalizes the conventional hierarchical access control paradigm, by extending it to certain additional sets of qualified users. Afterward, we propose two constructions for hierarchical key assignment schemes in this new model, which are provably secure with respect to key indistinguishability. In particular, the former construction relies on both symmetric encryption and perfect secret sharing, whereas, the latter is based on public-key threshold broadcast encryption.

R18

A secret sharing scheme is a method to store information securely and reliably. Particularly, in a threshold secret sharing scheme, a secret is encoded into n shares, such that any set of at least t1 shares suffice to decode the secret, and any set of at most $t2 < t1$ shares reveal no information about the secret. Assuming that each party holds a share and a user wishes to decode the secret by receiving information from a set of parties; the question we study is how to minimize the amount of communication between the user and the parties. We show that the necessary amount of communication, termed "decoding bandwidth", decreases as the number of parties that participate in decoding increases. We prove a tight lower bound on the decoding bandwidth, and construct secret sharing schemes achieving the bound. Particularly, we design a scheme that achieves the optimal decoding bandwidth when d parties participate in decoding, universally for all $t1 \leq d \leq n$. The scheme is based on a generalization of Shamir's secret sharing scheme and preserves its simplicity and efficiency. In addition, we consider the setting of secure distributed storage where the proposedcommunicationefficientsecretsharingschemesnotonly improve decoding bandwidth but further improve disk access complexity during decoding

R19

QR barcodes are used extensively due to their beneficial properties, including small tag, large data capacity, reliability, and high-speed scanning. However, the private data of the QR barcode lacks adequate security protection. In this article, we design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. The proposed approach differs from related QR code schemes in that it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation. The secret can be split and conveyed with QR tags in the distribution application, and the system can retrieve the lossless secret when authorized participants cooperate. General browsers can read the original data from the marked QR tag via a barcode reader, and this helps reduce the security risk of the secret. Based on our experiments, the new approach is feasible and provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode.

R20

Machine-to-machine (M2M) communication, an automated communications technology for equipment or devices, holds great promise in every corner of modern society, such as civil transportation, smart homes, smart grids and industrial automation. M2M technology is still in its infancy, and further development and deployment of M2M systems hinges on establishing an efficient and secure information management system with a satisfactory security level. In this paper, we extend the idea of (t,n) secret sharing for information transmission in M2M with high security and efficiency. Specifically, a secret is divided into 2k shares and then transmitted through 2k node-disjoint paths constructed by Latin square. Note that in our scheme, the secret key is simultaneously transmitted along with the encrypted message through these 2k paths from the source node to the destination node, which greatly improves the efficiency of pointto-point communications in M2M systems. Furthermore, owing to the properties of (t,n) secret sharing, the security of M2M communications is guaranteed. In addition, to avoid dishonest participants, verifiable secret sharing (VSS) is supported in the proposed scheme. Sufficient theoretical proof and performance analysis demonstrate that our scheme is secure and efficient for M2M communications.

R21

Preserving data confidentiality in clouds is a key issue. Secret Sharing, a cryptographic primitive for the distribution of a secret among a group of n participants designed so that only subsets of shareholders of cardinality $0 < t \leq n$ are allowed to reconstruct the secret by pooling their shares, can help mitigating and minimizing the problem. A desirable feature of Secret Sharing schemes is cheater detection, i.e. the ability to detect one or more malicious shareholders trying to reconstruct the secret by obtaining legal shares from the other shareholders while providing them with fake shares. Verifiable Secret Sharing schemes solve this problem by allowing shareholders verifying the others' shares. We present new verification algorithms providing arbitrary secret sharing schemes with cheater detection capabilities, and prove their space efficiency with regard to other schemes appeared in the literature. We also introduce, in one of our schemes, the Exponentiating Polynomial Root Problem (EPRP), which is believed to be NP-Intermediate and therefore difficult.

R22

In this paper, a class of two-weight and three-weight linear codes over GF(p) is constructed, and their application in secret sharing is investigated. Some of the linear codes obtained are optimal in the sense that they meet certain bounds on linear codes. These codes have applications also in authentication codes, association schemes, and strongly regular graphs, in addition to their applications in consumer electronics, communication and data storage systems.

R23

In this paper, we construct a lattice based (t,n) threshold multi-stage secret sharing (MSSS) scheme according to Ajtai's construction for one-way functions. In an MSSS scheme, the authorized subsets of participants can recover a subset of secrets at each stage while other secrets remain undisclosed. In this paper, each secret is a vector from a t-dimensional lattice and the basis of each lattice is kept private. A t-subset of n participants can recover the secret(s) using their assigned shares. Using a lattice based oneway function, even after some secrets are revealed, the computational security of the unrecovered secrets is provided against quantum computers. The scheme is multi-use in the sense that to share a new set of secrets, it is sufficient to renew some public information such that a new share distribution is no longer required.Furthermore,theschemeisverifiablemeaningthattheparticipantscanverifythesharesreceived from the dealer and the recovered secrets from the combiner, using public information.

R24

Shamir's secret sharing scheme is an effective way to distribute secret to a group of shareholders. The security of the unprotected sharing scheme, however, can be easily broken by cheaters or attackers who maliciously feed incorrect shares during the secret recovery stage or inject faults into hardware computing the secret. In this paper, we propose cheater detection and identification schemes based on robust and algebraic manipulation detection (AMD) codes and m-disjunct matrices (superimposed codes). We present the constructions of codes for cheater detection and identification and describe how the cheater identification problem can be related to the classic group testing algorithms based on m-disjunct matrices. Simulation and synthesisresultsshowthattheproposedarchitecturecanimprove the security level significantly even under strong cheating attack models with reasonable area and timing overheads.

R25

A basic (t,n)-secret sharing (SS) scheme allows a secret s to be divided into n shares and shared among n shareholders. In the scheme, any t or more than t shareholders can recover the secret while fewer than t shareholders cannot obtain the secret s. But an adversary without any valid share may obtain the secret if there are over t participants in the secret reconstruction. To address this type of attack, 1) we first introduce the notion of Randomized Component (RC), which binds a share with all participants and protects the share from being exposed to outside without any computational assumption; at the same time, RCs can be used to reconstruct the secret. 2) As one of the applications of RCs, a (t,m,n)-Group Oriented SS scheme is proposed to cope with the attack in basic (t,n)-SSs, in which once m (t m) participants form a tightly couple group by generating RCs, the secret can be recovered only if all m RCs are correct, which requires each participant to have a valid share in advance. Moreover, the scheme can secure the secret without any user authentication or share verification. Analyses show the proposed (t,m,n)-Group Oriented SS is asymptotically perfect and unconditionally secure. RCs can also be applied to build other schemes in a simple way, such as multi-secret sharing, group authentication and so on.

R26

Visual cryptography is a special type of secret sharing. Two models of visual cryptography have been independently studied: 1) deterministic visual cryptography, introduced by Naor and Shamir, and 2) random grid visual cryptography, introduced by Kafri and Keren. In this paper, we show that there is a strict relation between these two models. In particular, we show thatto any random grid scheme corresponds a deterministic scheme and vice versa. This allows us to use results known in a model also in the other model. By exploiting the (many) results known in the deterministic model, we are able to improve several schemes and to provide many upper bounds for the random grid model and by exploiting some results known for the random grid model, we are also able to provide new schemes for the deterministic model. A side effect of this paper is that future new results for any one of the two models should not ignore, and in fact be compared with, the results known in the other model.

R28

Most visual secret sharing (VSS) schemes need to encrypt a pixel of the secret image into m subpixels on the share; obviously, the shares are enlarged and so are the stacked images. A handful of studies try to solve the problem of pixel expansion, but little information is available on improving the visual effect of the stacked image. In addition, most of them do not mention how to deal with grey-level images. Since the secret is decoded by the human eye, the visual effect of the stacked image is an important issue in the study of the VSS scheme. This paper proposes two visual cryptographic methods to solve the problem of pixel expansion and to improve the visual effect of the stacked image at the same time. Unlike in previous studies, multiple pixels are simultaneously encoded each time. With the help of halftoning, the methods can be applied to encoding grey-level images. The experimental results show that these methods have a better visual effect on the stacked image compared with other researchers' methods. The methods are based on two basis matrices and hence can satisfy the security and contrast conditions required by the VSS scheme.

R29

Random grid (RG) is a method to implement visual cryptography (VC) without pixel expansion. However, a reconstructed secret with lower visual quality reveals in RG-based VC due to the fact that average light transmission of a share is fixed at .Inthiswork,weintroducetheconceptofgeneralizedRG, where the light transmission of a share becomes adjustable, and adopt generalized RG to implement different VC schemes. First, a basic algorithm, a generalized RG-based VC, is devised. Based on the scheme, two VC schemes including a generalized RG-based VC and a XOR-based meaningful VC are constructed. The two derived algorithms are designed to solve different problems in VC. In the scheme, recovered image quality is further improved. In the method, meaningful shares are constructed so that the management of shadows becomes more efficient, and the chance of suspicion on secret image encryption is reduced. Moreover, superior visual quality of both the shares and recovered secret image is achieved. Theoreticalanalysisandexperimentalresultsareprovidedaswell, demonstrating the effectiveness and advantages of the proposed algorithms.

R30

A visual cryptography scheme (VCS) is a kind of secretsharingschemewhichallowstheencodingofasecretimage into shares distributed to participants. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS). In this paper, we propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded EVCS. Experimental results compare some of the well-known EVCSs proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCSs in the literature. In addition, it has many specific advantages against these well-known EVCSs, respectively

R31

Two common drawbacks of the visual cryptography scheme (VCS) are the large pixel expansion of each share image andthesmall contrastoftherecoveredsecretimage. Inthispaper, we propose a step construction to construct VCSand VCSfor general access structure by applying (2,2)-VCS recursively, where a participant may receive multiple share images. The proposed step construction generates VCSand VCSwhich have optimal pixel expansion and contrast for each qualified set in the general access structure in most cases. Our scheme applies a technique to simplify the access structure, which can reduce the average pixel expansion (APE) in most cases compared with many of the results in the literature. Finally, we give some experimental results and comparisons to show the effectiveness of the proposed scheme.

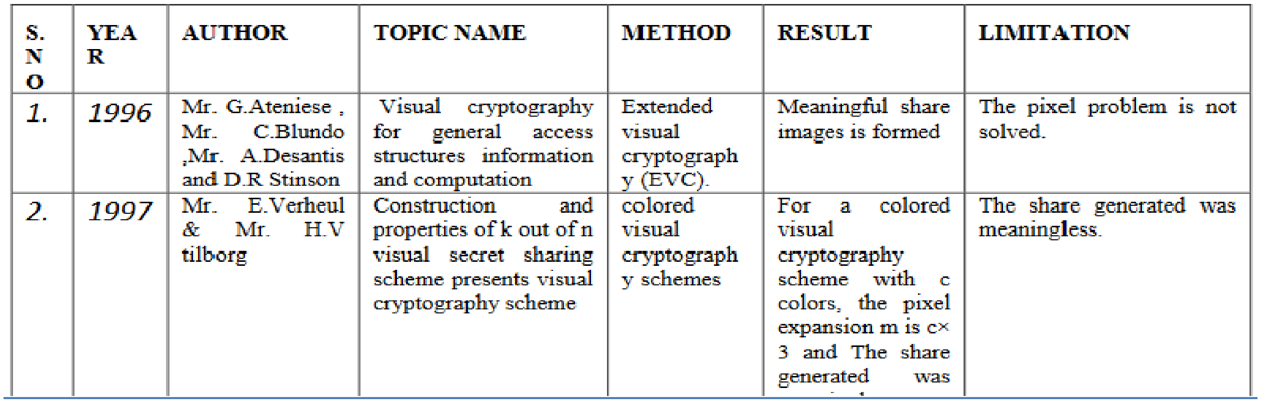
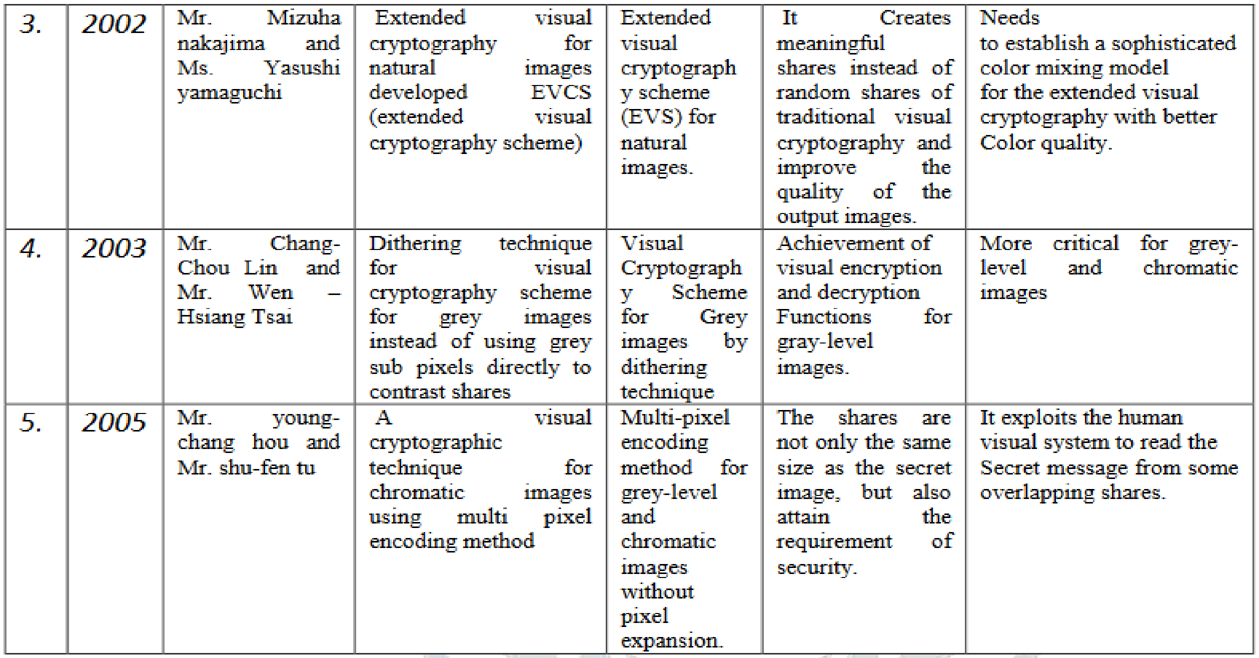
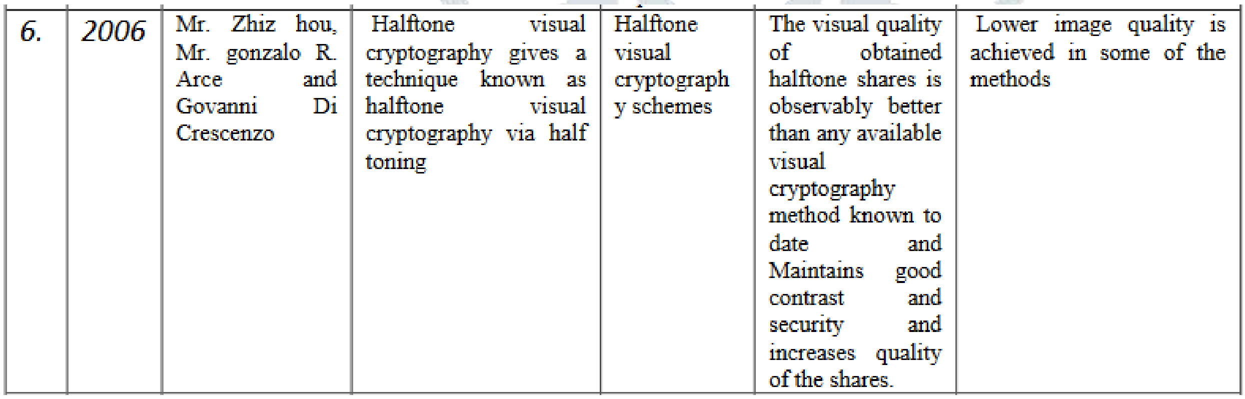
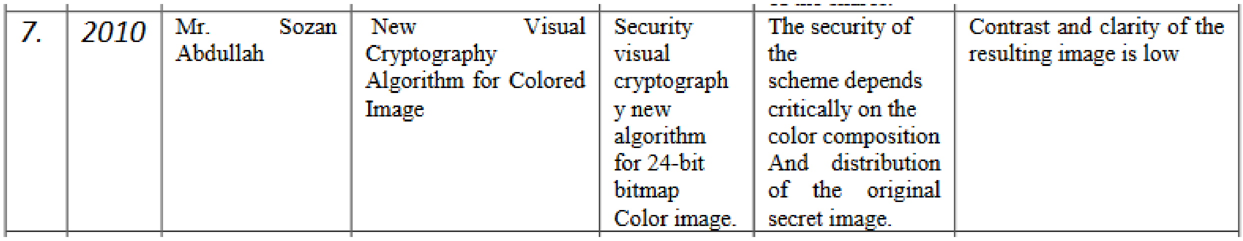
R32

Halftone visual cryptography (HVC) enlarges the area of visual cryptography by the addition of digital halftoningtechniques.Inparticular,invisualsecretsharingschemes,asecret image can be encoded into halftone shares taking meaningful visual information. In this paper, HVC construction methods based on error diffusion are proposed. The secret image is concurrently embedded into binary valued shares while these shares are halftoned by error diffusion—the workhorse standard of halftoning algorithms. Error diffusion has low complexity and provideshalftonesshareswithgoodimagequality.Areconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images. Factors affecting the share image quality and the contrast of the reconstructed image are discussed. Simulation results show several illustrative examples.

R33

A random grid in this paper is a transparency comprising a two-dimensional array of pixels that are either transparent or opaque determined in a totally random way. We design algorithms by using random grids to accomplish the encryption of the secret gray-level and color images in such a way that neither of the two encrypted shares alone leaks the information of the secret image, whereas the secret can be seen when these two shares are superimposed. The decryption process is done by our visual system and no

TABLE: Year wise review of different papersaccordingto their methods, resultsand limitations.

S. N O	YEA R	AUTHOR	TOPIC NAME	METHOD	RESULT	LIMITATION
1.	1996	Mr. G.Ateniese , Mr. C.Blundo ,Mr. A.Desantis and D.R Stinson	Visual cryptography for general access structures information and computation	Extended visual cryptography (EVC).	Meaningful share images is formed	The pixel problem is not solved.
2.	1997	Mr. E.Verheul & Mr. H.V tilborg	Construction and properties of k out of n visual secret sharing scheme presents visual cryptography scheme	colored visual cryptography schemes	For a colored visual cryptography scheme with c colors, the pixel expansion m is c× 3 and The share generated was	The share generated was meaningless.
3.	2002	Mr. Mizuha nakajima and Ms. Yasushi yamaguchi	Extended visual cryptography for natural images developed EVCS (extended visual cryptography scheme)	Extended visual cryptography scheme (EVS) for natural images.	It Creates meaningful shares instead of random shares of traditional visual cryptography and improve the quality of the output images.	Needs to establish a sophisticated color mixing model for the extended visual cryptography with better Color quality.
4.	2003	Mr. Chang-Chou Lin and Mr. Wen – Hsiang Tsai	Dithering technique for visual cryptography scheme for grey images instead of using grey sub pixels directly to contrast shares	Visual Cryptography Scheme for Grey images by dithering technique	Achievement of visual encryption and decryption Functions for gray-level images.	More critical for grey-level and chromatic images
5.	2005	Mr. young-chang hou and Mr. shu-fen tu	A visual cryptographic technique for chromatic images using multi pixel encoding method	Multi-pixel encoding method for grey-level and chromatic images without pixel expansion.	The shares are not only the same size as the secret image, but also attain the requirement of security.	It exploits the human visual system to read the Secret message from some overlapping shares.
6.	2006	Mr. Zhiz hou, Mr. gonzalo R. Arce and Govanni Di Crescenzo	Halftone visual cryptography gives a technique known as halftone visual cryptography via half toning	Halftone visual cryptography schemes	The visual quality of obtained halftone shares is observably better than any available visual cryptography method known to date and Maintains good contrast and security and increases quality of the shares.	Lower image quality is achieved in some of the methods
7.	2010	Mr. Sozan Abdullah	New Visual Cryptography Algorithm for Colored Image	Security visual cryptography new algorithm for 24-bit bitmap Color image.	The security of the scheme depends critically on the color composition And distribution of the original secret image.	Contrast and clarity of the resulting image is low

8.	2011	Mr. N Krishna Prakash, Member, IACSIT and Mr. S Govindaraju	Visual Cryptography Scheme for Color Images Using Half Toning Via Direct Binary Search with Adaptive Search and swap	Halftoning via Error Diffusion, Visual Secret Sharing Scheme, HALFTONE VISUAL CRYPTOGRAPHY FOR COLOR IMAGES,	1).Better quality of halftone image and the revealed secret, 2). Holds good for multiple colored image also, 3) Does not require any additional computational complexity.	Quality of halftone image Computational Complexity
9.	2012	Mr. John Justin .M and Alagendran.B and Mr. Manimurugan.S	A Survey on Various Visual Secret Sharing Schemes with an Application presents different kinds of visual secret sharing techniques	Visual secret sharing (VSS).	Visual secret sharing technique will always useful mainly in terms of security issues scheme	Some techniques are sensible, because they suit for appropriate places but not in all the places.
10.	2012	Mr. Anshul Sharma	Performance of error filters in halftone visual cryptography	Visual secret sharing scheme, halftone visual cryptography, error diffusion.	Visual quality of the halftone shares increases with the complexity Of the error filters.	Image quality of halftone shares
11.	2013	Mr. Sonal wange	A Visual Cryptography to Secure Biometric Database	Black And White Visual Cryptography Scheme , Color Visual Cryptography Schemes, Biometric identification technique	Perfectly secure method of keeping images secret, for feasible use in biometric identification technique and protection such as fingerprint images	Visual Cryptography is used with short messages.
12.	2014	Mr. Manjula D. C.,Vijaya C	Novel Encryption method for Grayscale Halftone Images using Random numbers	(2,2) VC scheme, Decryption ,encryption algorithm	The proposed scheme is highly Secured, and the quality of the reconstructed image is good.	Affects the contrast of the resulting image.
13.	2014	Mr. Mona F. M. Mursi ,May Salama and Manal Mansour	Visual Cryptography Schemes: A Comprehensive Survey	Visual cryptography schemes (VCS), Extended Visual Cryptography (EVC), Key Based VC	Improved visual quality of the retrieved image.	The shares were still meaningless

14.	2014	Mr. Prateek Kumar, Ms. Suneeta Agarwal and Mr. Shivendra Shivani	Halftone visual cryptography with pixel expansion through error diffusion presents extended visual cryptography(EVC) concept	Error diffusion, halftone visual cryptography, Half toning visual cryptography, Image processing, secret sharing	We get good quality and better contrast image with pixel expansion	Recovered image has degradation in visual quality
15.	2015	Mr. Nazimul islam and Ms. shaloo kikan	A Survey: Novel Study for Visual Cryptography in Discrete Wavelet Transforms presents visual cryptography scheme (VCS)	(2, 2) Visual Cryptography Scheme , Halftone Visual Cryptography, Visual Cryptography for scan and print applications, Recursive Threshold visual cryptography	Wavelet based can effectively minimize transmission risk and provide the highest level of user friendliness, both for shares and for participants.	The shares produced by all the methods above are either meaningless or are dependent upon some factors like the number of colors in the secret image.
16.	2015	Mr. Ritesh D.Yelane, Dr. Nitiket. N. Mhala and Prof. B. J. Chilke	Security Approach by Using Visual Cryptographic Technique	Embedded Extended Visual Cryptography Scheme, Secret Sharing, Half toning, Privacy and security, EVCS.	Improved contrast of the recovered secret image and produce clear resultant image.	Information security Contrast
17.	2016	Ms. Shruti .M. Rakhude and Ms. Manisha Gedam	Survey on Visual Cryptography: Techniques, Advantages and Applications	Visual Cryptographic Schemes for Black and White Images / Binary Images , Visual Cryptography Schemes for color images.	Various applications systems can be made more secure and reliable by the application of visual cryptography techniques.	Only one secret could be hidden using this technique.

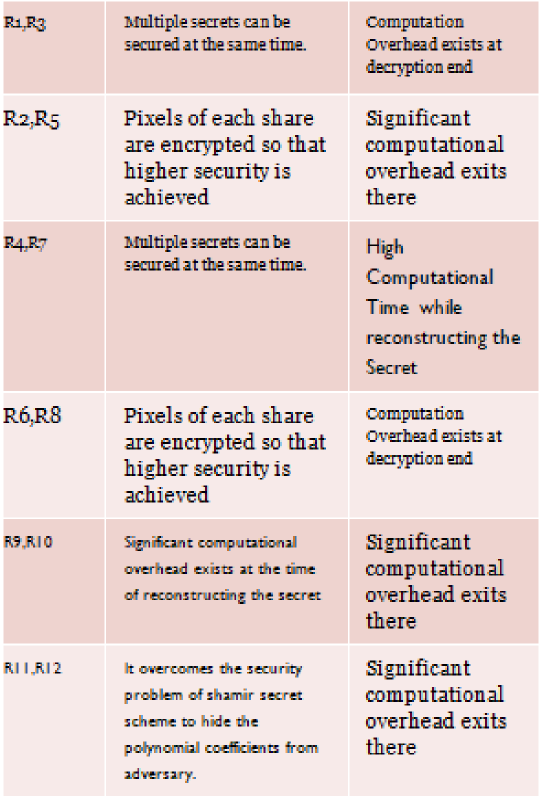
18.	2016	Mr. T. Ambritha, Mr. J. Poorani Sri and Mr. J. Jessintha Jebarani and Mr. M. Pradhiba Selvarani	Comparative Study of Various Visual Cryptography Techniques	Region Incremental Visual Cryptography, Visual Cryptography Scheme (with Random Key), (2, 2) Visual Cryptographic Scheme, Digital Watermarking	poor RIVC ,Good VCS (with Random Key),Fair (2,2)VCS and Digital Watermarking.	The quality of the image was degraded because of half toning and The recent research works well for text, logos but for color image and Gray scale image it works average.

JETIR

computation is required. As compared to the approaches in visual cryptography, our algorithms do not need the basis matrices to encode the shares so that the problem of pixel expansion exists no more; that is, the sizes of the secret image and the encrypted shares are the same

.

III. Issues and Challenges



R1,R3	Multiple secrets can be secured at the same time.	Computation Overhead exists at decryption end
R2,R5	Pixels of each share are encrypted so that higher security is achieved	Significant computational overhead exits there
R4,R7	Multiple secrets can be secured at the same time.	High Computational Time while reconstructing the Secret
R6,R8	Pixels of each share are encrypted so that higher security is achieved	Computation Overhead exists at decryption end
R9,R10	Significant computational overhead exists at the time of reconstructing the secret	Significant computational overhead exits there
R11,R12	It overcomes the security problem of shamir secret scheme to hide the polynomial coefficients from adversary.	Significant computational overhead exits there

Figure:- Method-Strength-Weakness

Challenges:-

1. **Large Computation Overhead during Reconstruction of Secret Image.**
2. **Large Pixel expansion and low contrast output**
3. **Maintenance of confidentiality, integrity, authenticity, and non-reputability of distinct shares**

IV. RESULTS

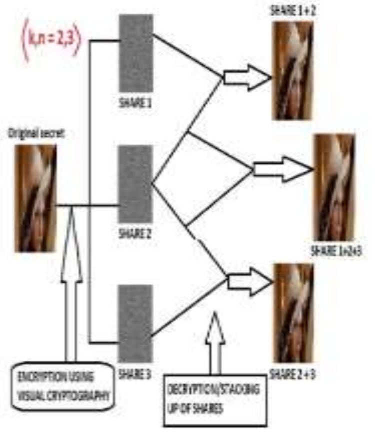


Fig. 1: Illustration of "(k, n) threshold" visual cryptography(VC) scheme

From the study of various visual cryptography scheme it was observed that this concept has made cryptography much easier to implement without using any complex keys. (k, n) threshold scheme has high pixel expansion while as progressive visual cryptography avoids this problem of pixel expansion. ISS using circular shares and its variants have also been studied. It gives an option of encoding images through rotation of an angle but it leads to loss of information and distortion in reconstruction phase as circular shares do not cover whole of an image for encoding. Visual cryptography with cloud and progressive VSS with perfect reconstruction help in zero contrast loss which results in the retrieval of secret perfectly. Table.1 gives the comparison between various visual cryptography techniques.

Sr. No.	Research Paper#	Method	Parameter and Dataset	Improvement
1	R1	We propose an analysis-by-synthesis (AbS) framework to integrate thehalftoning process and the VC encoding.	Visual Quality, Medical Images Dataset	Aiming at improving the visual quality of the reconstructed secret image (i.e., target image) in size-invariant visual cryptography,
2	R2	This paper aims to improve the usefulness of the d-MSS by enhancing the security against malicious adversaries.	Security of Shares, Satellite Images Dataset	private secret sharing schemes can be constructed
3	R3	Our main result establishes a family of bounds which are tighter than previously known bounds	Minimum No. of shares, Industrial Image Dataset	we make the following remark on the asymptotic behaviors of the partial privacy and reconstruction thresholds
4	R4	we propose a new technique by using multi-secret sharing as the underlying encryption	multi-secret sharing, Process Flow Images Dataset	new class of reversible data hiding in encrypted images

5	R5	In this paper, we have connected the additive and monotonic nature of memristor devices with secret sharing-based user authentication ideas	Computational efficiency and Security, Binary Images Dataset	under realistic attacking assumptions, the proposed protocols are secure and it is computational eficcient
6	R8	An important problem in secret sharing schemes is minimizing the share size	Share Size, MotherBoard Images Datataset	we presented an optimal construction of USS schemes, which makes the entropy of each share equal to the derived lower bound.
7	R9	we propose a visual secret sharing scheme to encode a secret QR code into several shares.	Data Storage and Security, Satellite Images Data set	Experimental results show that the proposed scheme is both feasible and reasonably secure
8	R13	The aim of this paper is to maximize the range of the access control of visual secret sharing (VSS) schemes encrypting multiple images	Muli-Secret and Access Control, Medical Images Data	It makes its security analysis simpler and more practical.
9	R18	we study is how to minimize the amount of communication between the user and the parties.	Communication Efficiency and share size, Process Flowchart Images Data Set	The scheme is simple and is efficient in both space and Computation
10	R24	We present the constructions of codes for cheater detection	Security, Satellite Images Data	Results show that the proposed method can increase the security level of the system and protect the system against strong cheaters

Table 1: Result analysis of some Research Papers

V. CONCLUSION AND FUTURE SCOPE

This paper presented a survey on various studies conducted in the areas of secret image sharing schemes. The secret image sharing features of the existing algorithms are carefully investigated in this paper. From the above investigations, it is found that each SIS scheme has its own merits, even though, there is a need to improve in terms of pixel expansion problems, loss of reconstruction accuracy, reconstruction complexity problem, low quality of the reconstructed image and diminished security of shadows all at the one time.

Many secret sharing techniques have been surveyed in this paper. Comparison was made on the factors and parameters already discussed. It was found out that a technique should have minimum pixel expansion, high security features, better contrast and algorithm should be simple. Progressive secret sharing scheme with perfect reconstruction provided a better contrast but algorithm was a bit complex. Traditional (k, n) visual cryptography had high pixel expansion but simpler to implement. Visual cryptography based on cloud is a novel technique that provides a perfect reconstruction and a better security. It is essential to concentrate on the fact that the shares that are generated should be completely different and while reconstruction of secret a high quality image is retrieved so that the secret information is not lost. There is a lot of scope in the field of visual cryptography in terms of providing more secure algorithms and at the same time being light weight and simple. It also enables secure transmission of images with data embedded into them. Data embedding is done in images using various secure techniques like hiding in encrypted images [33], data hiding in scrambled images as described in [34], etc. Using concept progressive ISS schemes bring in a lot easiness in construction of shares. It also makes algorithms more simple and secure. It enables us to develop as many shares as possible with any limitation of pixel expansion. Different features of progressive ISS algorithms can be studied and combined with the concept of cloud so that a more secure algorithm is developed without any of the above mentioned drawbacks.

Objectives :-

1) **Keeping the share size not greater than the original image**

2) **Providing secrecy to shares so that no malicious user can't reconstruct secret image**

3) **Negligible Computation Overhead during reconstruction of secret image**

REFERENCES

1. Bin Yan, Yong Xiang and GuangHua "Improving the Visual Quality of Size-Invariant Visual Cryptography for GrayscaleImages:An Analysis-by-Synthesis (AbS) Approach", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 28, NO. 2, pp.896 – 911,FEBRUARY 2019.
2. Maki Yoshida and Satoshi Oban, "Verifiably Multiplicative Secret Sharing", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 65, NO. 5, pp. 3233 – 3245,MAY 2019.
3. Ignacio Cascudo, JaronSkovstedGundersen and Diego Ruano, "Improved Bounds on the Threshold Gap in Ramp Secret Sharing", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 65, NO. 7, pp. 4620 – 4633, JULY 2019.
4. Yu-Chi Chen, Tsung-Hsuan Hung, Sung-Hsien Hsieh, and Chih-Wei Shiu, "A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms", pp.3332 - 3343, May 2019.
5. MdTanvirArafin and Gang Qu, "Memristors for Secret Sharing-Based Lightweight Authentication", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, 2671 – 2683, April 2018.

6. Zhili Zhou, Ching-Nung Yang, Yi Cao, “Secret Image Sharing based on Encrypted Pixels”, pp. 15021 – 15025, , in IEEE Access, March 2018.
7. Ankit Singh Rawat, O. OzanKoyluoglu and SriramVishwanath, “Centralized Repair of Multiple Node Failures with Applications to Communication Efficient Secret Sharing”, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 64, NO. 12, pp. 7529 – 7550, September 2018.
8. Mohammad Reza KhaliliShoja, George T Amariucai, Zhengdao Wang, Shuangqing Wei, Jing Deng, “On the Secret Key Capacity of Sibling Hidden Markov Models”, IEEE Transactions on Information Forensics and Security, pp. 1556-6013, July 2018.
9. Maki Yoshida, Toru Fujwiara and Marc P.C. Fossorier, “Optimal Uniform Secret Sharing”, DOI 10.1109/TIT.2018.2852276, IEEE Transactions on Information Theory, pp. 436 – 443, November 2018.
10. Yuqiao Cheng, Zhengxin Fu, Bin Yu, “Improved Visual Secret Sharing Scheme for QR Code Applications”, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Information Forensics and Security, pp. 2393 – 2403, March 2018.
11. Umberto Mart´ ınez-Pe˜ nas, “Communication efficient and strongly secure secret sharing schemes based on algebraic geometry codes”, IEEE Transactions on Information Theory pp. 4191 - 4206 , April 2018.
12. Xueqing Gong, Ping Hu, Kenneth W. Shum and Chi Wan Sung, “A Zigzag-Decodable Ramp Secret Sharing Scheme”, IEEE Transactions on Information Theory, pp. 1906 – 1916,February 2018.
13. Manami Sasaki and Yodai Watanabe, “Visual Secret Sharing Schemes Encrypting Multiple Images”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 13, NO. 2, pp. 356 – 365, FEBRUARY 2018.
14. Ching-Nung Yang, Chih-Cheng Wu, and Yi-Chin Lin, “k out of n Region-Based Progressive Visual Cryptography”, IEEE Transactions on Circuits and Systems for Video Technology, pp. 252 – 262, November 2017.
15. Zahra Ahmadian, SadeghJamshidpour, “Linear Subspace Cryptanalysis of Harn’s Secret Sharing-Based Group Authentication Scheme”, IEEE Transactions on Information Forensics and Security, pp. 502 – 510, September 2017.
16. Long Bao, Shuang Yi and Yicong Zhou, “Combination of sharing matrix and image encryption for lossless (k; n)-secret image sharing”, IEEE Transactions on Image Processing, pp. 5618 – 5631, August 2017.
17. Arcangelo Castiglione, Alfredo De Santis, Barbara Masucci, Francesco Palmieri, Aniello Castiglione, Jin Li, and Xinyi Huang, “Hierarchical and Shared Access Control”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 4, pp. 850 – 865, APRIL 2016.
18. Wentao Huang, Michael Langberg, JoergKliewer, and JehoshuaBruck, “Communication Efficient Secret Sharing”, IEEE Transactions on Information Theory, pp. 7195 – 7206, October 2016.
19. Pei-Yu Lin, “Distributed Secret Sharing Approach with Cheater Prevention based on QR Code”, IEEE Transactions on Industrial Informatics, pp. 384 – 392, January 2016.
20. JianShen, Tianqi Zhou, Xingang Liu, Yao-Chung Chang, “A Novel Latin Square-based Secret Sharing for M2M Communications”, IEEE Transactions on Industrial Informatics, VOL. 14, NO. 8, pp. 3659 – 3668, AUGUST 2015.
21. Massimo Cafaro and Piergiuseppe Pell”, Space-efficient Verifiable Secret Sharing Using Polynomial Interpolation”, IEEE Transactions on Cloud Computing, pp. 453 – 463, January 2015.
22. Kelan Ding and Cunsheng Ding, “A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing”, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 61, NO. 11, pp. 5835 – 5842, NOVEMBER 2015.
23. HosseinPilaramTaranehEghlidos, Tehran, Iran”, An Efficient Lattice Based Multi-stage Secret Sharing Scheme”, IEEE Transactions on Dependable and Secure Computing, pp. 2 – 8, May 2015.
24. Zhen Wang, Mark Karpovsky and Lake Bu, “Design of Reliable and Secure Devices Realizing Shamir’s Secret Sharing”, IEEE Transactions on Computers, pp. 2443 – 2455, October 2015.
25. Miao FuyouXiong Yan Wang XingfuMoamanBadawy, “Randomized Component and Its Application to (t,m,n)-Group Oriented Secret Sharing”, IEEE Transactions on Information Forensics and Security, pp. 889 – 899, December 2014.
26. Grid and Its Applications in Visual Cryptography”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 9, pp. 1541 – 1553, SEPTEMBER 2013.
27. Feng Liu and Chuankun Wu, “Embedded Extended Visual Cryptography Schemes”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, pp. 307 – 322, JUNE 2011.
28. Feng Liu, Chuankun Wu, Senior Member, IEEE, and Xijun Lin, “Step Construction of Visual Cryptography Schemes”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 1, pp. 27 – 38, MARCH 2010.
29. Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo, “Halftone Visual Cryptography Via Error Diffusion”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, pp. 383 – 396, SEPTEMBER 2009.
30. ShyongJianShyu, “Image encryption by randomgrids”, Pattern Recognition,vol. 40 pp. 1014 – 1031, March 2007.
31. Yung-Fu Chen, Yung-Kuan Chan, Ching-Chun Huang, Meng-Hsiun Tsai, Yen-Ping Chu, “A multiple-level visual secret-sharing scheme without imagesize expansion”, Information Sciences, vol. 177, pp. 4696–4710, Nov. 2007.
32. Ching-Nung Yang, “New visual secret sharing schemes using probabilistic method”, Pattern Recognition Letters, vol. 25, pp. 481-494, March 2004.It provides better privacy