A SURVEY ON TECHNIQUES FOR REVERSIBLE DATA HIDING

[1]Anumsamreen Patel, [2]Ravi Hosur, [3]Anand Hiremath
[1]PG Student, [2]Asst. Professor, [3]Asst. Professor
[1,2,3]Department of Computer Science and Engineering
[1,2,3]B.L.D.E.A's V. P. Dr. P. G. Halakatti College of Engineering and Technology, (Affiliated to Visvesvaraya Technological University, Belagavi-590018)
Vijayapur-586101, India.

Abstract: This paper presents a survey on the broadly available techniques for data hiding. Essentially, it is defined as hiding or protecting classified data or information from unauthorized or unintended access. Each of these methods have their respective disadvantages and their fair share of advantages as well. Among the techniques mentioned in this paper some of them give more focus to robustness, and some focus on the hiding of data itself efficiently while some focus on the capacity of the data that has to be embedded. The primary objective is to get to get one or more than one of these concerns taken care of. The work related to the techniques that have been used so far for this purpose has been described in this paper along with improvements that can be used to overcome the limitations of other methods.

Index Terms **– steganography, cryptography, watermarking, AES.**

I. Introduction

Everything is being digitized in the present days, ranging from banking to shopping, bills to communication. Given this hype, the integrity, security and confidentiality of the information or data flowing through these various media cannot be entrusted to traditional methods for safety and security. So, there are new techniques proposed all these years in order to impart security and safe transmission to data across the respective digital medium. They include combinations of watermarking, cryptography, and steganography. These techniques have their own goals to achieve and their own problems to overcome. Mainly they depend on the domain in which they are used and the digital images are manipulated. Both cryptography and the watermarking are associated techniques but watermarking in itself, is discrete [1] from the cryptography. Mainly what they do is embed the host data with the desired one and then transmit it [2]. Watermarking is mainly used in copyright protection.

II. Related Works

Different kinds of techniques proposed broadly for hiding of data are explained here.

The first method considers embedding medical images with the patient information, and this was proposed by Moniruzzaman et al. in paper [3]. This technique is a win if we consider the image quality as the driving factor for the technique. Initially used, is a discrete wavelet transform, which is applied on to considered image, to get four coefficient sets which do not overlap 00,01,10,11, which are multiresolution. The lowest 00 is divided into 3*3 blocks which are not overlapping as well. Then the grey level difference is calculated between the neighbor and center pixel taking the central one as threshold and assigning them their values accordingly. And then XOR is applied in order to create a map of logistics another XOR is applied to the watermarked image and the map in order to obtain the bits of watermark which are chaotic and embed them into lowest band with the conditions of neighboring pixels in mind. To obtain the original image an inverse discrete wavelet transform is utilized. Considerable advantage that this method offers, is a fine peak signal to noise ratio and quality to both image and watermark.

Sukhpal et al. in the paper [4], uses upgraded HAAR discrete wavelet transform and repetitive generation two discrete wavelet transform packets to decompose the actual image into sub images to a size of fourth time the image which is watermarked. Then the repetitive transformation is applied to the final decomposition to provide a satisfactory level of security in the pixels which belong to image which is watermarked. The grey scale values are computed, and their division is done in three parts X, Y and Z. The sub images are again divided into four more bands then they are equal in size to the water mark and they along with X, Y and Z are incorporated into the remaining leaving the first one. Now the entire thing is incorporated into the repetitive discrete wavelet transform packet and this makes the watermark close to invisible. This scheme is highly robust but it is very complex and has a large processing time.

In the next technique, Gayathri et al in the paper [5] proposes a technique to merge the features provided by watermarking, steganography , and cryptography to divide an image which is in binary format into blocks of 8*8 and each of these blocks is applies with a zigzag sequence of hiding to make it difficult to guess the path of data hiding. After that a {2,2} VC share method is used to create an encrypted form of the image. The benefit of this particular scheme is that it wins if the quality of the considered image is major concern, but it has massive processing times due to the fact that algorithms which use steganography are very complex indeed.

Jasdeep et al. in the paper [6] used the Blowfish algorithm to nest the technique of watermarking and then carry out the encryption. This algorithm divides the data into specified length blocks whose length can be anywhere from 32 to 448 in terms of bits. In this method two watermarks are created, the first one which is a dummy is encrypted using the blow fish and it is fed into the second one which is the actual watermark. Increased data accommodation is an advantage provided by this method along with its robust nature.

Yanyan et al. in the paper [7], also suggested the use of visual cryptography along with (DCT) abbreviated discrete cosine transform to produce two shares. One is incorporated into the coefficient of discrete cosine transform, and the other in the colour image, preferably in the component blue. The remaining share is guarded by copyright. Here, the two shares are generated using visual cryptography (2,2) and XOR. The component of the colour image is isolated to form 8*8 block which are not overlapping. First share is incorporated, and an inverse discrete wavelet transform is utilized on, to get the actual image which is watermarked. This scheme is less complex but the peak signal to noise ratio that it offers is not as good.

Similar technique offered to medical digital images was introduced by Nassiri et al. in the paper [8]. According to this technique, the image is changed into the frequency domain from the space domain by making utilizing discrete wavelet transform L{L=4}. After this, a pseudo mask which is easily detectible as added in order to divert attention from the original watermark, it is easily detectible therefore acts as a dummy. Let's denote watermark with **W**, here they use a pseudo random method to generate a binary sequence, and then encryption of **W** is carried out using the generated pseudo random vector (binary) and then W* is generated. This is embedded inside the image in play. Then, inverse discrete wavelet transform is utilized to get the image which is marked. Advantage with this method is we can get high quality images and it is not sensitive to certain filters but the robustness is in question as it depends on the alpha value.

Sanjay Kumar et al. in the paper [9] proposes using block entropy which is mainly used for authenticating and protection of copyrights in the digital images. According to this method, the entropy of actual image is calculated first, carrying out division of the considered image in 64 blocks, and computing their entropies. Then, the image which is water marked is resized to be equal to the size of blocks of the actual image and then it is incorporated into those blocks. This technique offers a satisfactory peak signal to noise ratio, but it is not very secure.

Mr. Ali et al. in the paper [10], proposed combination of water marking and cryptography. This scheme was proposed for medical images. The scheme suggests dividing the image into two parts first part is the part of interest and the second is the part of non interest. A third level discrete wavelet transform is used on the second part and the water marks are also of three types integrity, tampering localization and authenticity. Two more are generated using the part of interest in the later stages. After this the image is equally decomposed in four parts which are sub bands. A second level discrete wavelet transform is applied to first of the four bands, and third level discrete wavelet transform is applied to the second band further dividing them into four more sub bands respectively. The data of the patient is embedded into the third band and after that, inverse discrete wavelet transform is done. This complex method provides invisibility and data security.

OUSLIM et al. in the paper [11], used quantization of vector and the Lloyd technique to embed the information of iris of the eye into the image of fingerprint which provided more security to both the images, both use their separate databases. Here, a permuted variety of water mark is created by using XOR on both the images mentioned earlier. The image of fingerprint is also divided into 2*2 sized blocks and then Lloyd is applied and get a quantized image I. The variance of quantized vector indices is generated to create a binary matrix of polarity M. A key is also generated using permutations. This method is a win terms of security and robust to attacks. Sudip Ghosh et al. in the paper [15], proposes a similar technique using extended hamming code instead of Lloyd technique.

Bakhtiari et al. in the paper [12] proposes cryptography bases on elliptical curve while doing the compression of jpeg image and after that as well. This method is extremely useful when power, storage and bandwidth are unfortunately limited. In the method, the elliptical cryptography is utilized with but independently to the being algorithm used for compression to get the encryption done. Here two types of algorithms are presented, one type of encryption is selective and the other is perceptual. Security and speed are the advantages provided by this scheme but a lot of changes to the codec are required during the elliptical cryptography.

Anusree et al. in the paper [13], uses visual cryptography for sharing multiple secrets. In the technique, the original image is divided into CMY components and halftoning is used on individual component. And then the VCS is used (2,2) to encode all the pixels. Which creates two shares for every CMY component named sheets. First share will be marked on first sheet and the second on second sheet. All shares are needed to get the original image. This method provided enhanced security but, it requires bigger storage and does not have a satisfactory peak signal to noise ratio. Gupta in the paper [14], proposes to increase the security of the mark itself. The proposed method seeks to provide an increased level of the security of the image in binary format. In this proposed method, the first watermark is embedded with the data using the operation XOR and the result is embedded in another watermark, the result is then embedded in the first again. This type of recursive scheme is used to create a watermark which is blind. Security is absolutely an advantage in this system, but the process is very complex, and the processing times are higher too.

Meeta Malonia at el. in the paper [17], proposes using arithmetic progression along with discrete wavelet transform, to increase the perceptibility and also increase robustness of the system. The actual image is transformed into a grey scale image whose size is 512*512 then, a second level discrete wavelet transform is used on it to get four sub bands which are repreented as 00,01,10,11. Then the QR code of the image is also transformed into grey scale, and then to binary whose size is equal to 48*48. This is considered to be the image which is water marked which is again subjected to change in size 1*1024 and later 3*768. Average of all the bands is computed, and these are incorporated in an ascending order. The 1*768 component is extracted and converted to 3*256. An equation is utilized to determine the places where the water mark is to be embedded. Arithmetic progression is used to do this further task of embedding. Lastly a second level inverse discrete wavelet transform is utilized to get the final image again. This technique provides high robust nature. And also wins in terms of perception. But this technique is very complex and requires higher processing times.

Table 1: Different works in comparison

Sl no.	Ref. no	Aim	Strategies used	Peak signal to noise ratio
1	[3]	Provide integrity of patient data and maintain good image quality	Creating a map of logistics using chaotic technique of watermarking and discrete wavelet transform.	can reach 49.5
2	[4]	Improve the quality of the embedded image.	Modified version of quick HAAR discrete wavelet transform.	can reach 55.1
3	[5]	Combine the advantaged provided by digital watermarking, cryptography and steganography resulting a high security.	VC (visual cryptographic technique), digital water marking)	can reach 55.9
4	[6]	Increase the capacity or amount of data which is considered as classified, that can be embedded in the image under consideration.	Blowfish technique and digital nested water marking	Not specified
5	[7]	Provide increased amount of data that can be embedded along with increased security to that data	Discrete cosine transforms along with visual cryptographic technique	can reach 42
6	[8]	Provide authenticity and fragility to primarily medical images using grey scale transformations.	Discrete wavelet transform, digital water marking. Random number generation.	can reach 38.28
7	[9]	Copyrights protection along with authentication of data	Block Entropy along with spatial domain water mark	can reach 69.2
8	[10]	Increase the security of images in medical field using a hybrid of techniques.	Third level discrete wavelet transform and three different types of water marks	can reach 98.1
9	[11]	Provide high security using discrete wavelet transform to individual red green blue components in image which is considered.	Decomposition of Red, Green and Blue components of the image and Discrete wavelet transform	can reach 61.62
10	[12]	Provide increased security and increased robustness by combining water marking with signature biometric	Quantization of vectors and Linde buzo grey algorithm	can reach 10
11	[13]	Providing high security to the JPEG format images using Elliptical curve of cryptography. Prior to and throughout compression.	Encryption based on elliptical curve of cryptography and quantization of discrete cosine transform. Prior to and throughout compression process	can reach 17.70
12	[14]	To provide security to central DBs which carry biometric information	Extended version of visual cryptographic techniques with halftoning	can reach 21.23

13	[15]	Provide high level security by nesting of one watermark in the other recursively.	Nested and recursive encryption and watermarking and discrete wavelet transform.	can reach Not specified
14	[16]	Design a blind technique of watermarking which offers self-correction along with authentication	Extended version of Hamming code	can reach 81.78

III. Limitations of the methods mentioned above

A combination of the necessary features is not seen in the above methods

- Some methods provide high security but compromise on the image quality.
- Some methods provide good non perceptibility of hidden data but could not provide necessary security.
- Some methods provide a good peak signal to noise ratio but are extremely complex.
- Some method provides simplicity but, are not as efficient or robust to attacks.

Improvements that can be done to overcome the drawbacks

- Use a method that is not considered to significantly affect the image quality, such as incorporating data into the least significant bits in the pixels in the image, such changes will at least, not be visible to naked eye.
- Use a technique that can incorporate more data and provide additional non-perceptibility such are dividing the image into two parts and incorporating the data separately for added security.
- Use an encryption technique which is effective and not too complex, hence reducing the processing time.

IV. Conclusion

This paper has its primary focus on different kinds of techniques employed for data hiding. Every technique has its own set of benefits and drawbacks which are suitable for various application domains. The aim of the majority of works mentioned in this paper is the achievement of two, at minimum of these following properties – high capacity of embedding, enhanced security, highly robust to attacks and non-perceptibility. Some of these are tradeoffs, that is, if we want one, we have to let go of the other. That is why we are in need of techniques which can provide maximum of these above-mentioned characteristics. At the end, some improvements are suggested which can possibly overcome the drawbacks to some extent. In the foreseeable future, there is scope to combine these above-mentioned techniques and develop an efficient technique which can easily be used with a network of limited bandwidth and limited computation power or capacity of batteries.

REFERENCES

[1] Mohan Durvey and Devshri Satyarthi,“A Review Paper on Digital Watermarking,” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, July-August 2014.
[2] Mohammad Abdullatif, Akram M. Zeki, Jalel Chebil and Teddy surya Gunawan,“Properties of Digital Image Watermarking,” IEEE 9th International Colloquium on Signal processing and its Applications, 8-10 Mac. 2013, kuala Lumpur, Malaysia.
[3] Md. Moniruzzaman, Md. Abul Kayum Hawlader and Md. Foisal Hossain,“Wavelet Based Watermarking Approach of Hiding Patient Information in Medical Image for Medical Image Authentication,” IEEE 17th International Conference on Computer and Information Technology (ICCIT),2014, pp.374-378.
[4] Sukhpal Kaur and Madan Lal, “An Invisible Watermarking Scheme Based on Modified Fast Haar Wavelet Transform and RSGWPT,” Proceedings of IEEE 2015 RAECS UIET Panjab University Chandigarh 21-22nd December 2015.
[5] R. Gayathri and Dr. V. Nagarajan,“Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme,” IEEE ICCSP conference, 2015, pp.0118-0123.
[6] Jasdeep Singh Bhalla and Preeti Nagrath, “Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm,” International Journal of Scientific & Engineering Research Publications, Volume 3, Issue 4, April 2013.
[7] Yanyan Han, Wencai He, Shuai Ji and Qing Luo,“A Digital Watermarking Algorithm of Colour Image based on Visual Cryptography and Discrete Cosine Transform” IEEE Ninth International Conference on P2P, Parallel Grid, Cloud and Internet Computing, 2014. pp. 527-530.
[8] B. Nassiri, R.Latif,A.Toumanari and F.M.R. Maoulainine, “Secure transmission of medical images by watermarking technique,” IEEE, 2012.
[9] Sanjay Kumar and Ambar Dutta“A Novel Spatial Domain Technique for Digital Image Watermarking Using Block Entropy” IEEE Fifth International Conference on Recent Trends in Information Technology, 2016.
[10] Ali Al-Haj, Noor Hussein and Gheith Abandah, “Combining Cryptography and Digital Watermarking for Secured Transmission of Medical Images” IEEE, 2016.
[11] Madhuri Rajawat and D S Tomar, “A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT,” IEEE Fifth International Conference on Communication Systems and Network Technologies, 2015, pp.638-642.

[12] Mohamed OUSLIM, Ahmed Sabri and Hassan MOUHADJER, “Securing biometric data by combining watermarking and cryptography” IEEE 2nd International Conference on Advances in Biomedical Engineering, 2013, pp. 179-182.
[13] Saeid Bakhtiari et al. in [5], “JPEG Image Encryption with Elliptic Curve Cryptography,” IEEE International Symposium on Biometrics and Security Technologies (ISBAST),2014, pp. 144-149.
[14] Anusree K and Dr Binnu G S “Biometric Privacy using Visual Cryptography, Halftoning and Watermarking for Multiple Secrets” IEEE, 2014.
[15] Preeti Gupta in, “Cryptography based digital image watermarking algorithm to increase security of watermark data,” International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012.
[16] Sudip Ghosh, Sayandip De, Santi Prasad Maity and Hafizur Rahaman, “A Novel Dual Purpose Spatial Domain Algorithm for Digital Image Watermarking and Cryptography Using Extended Hamming Code” IEEE Proceedings of International Conference on Electrical Information and Communication Technology (EICT 2015), 2015, pp. 167-172
[17] Meeta Malonia and Surendra Kumar Agarwal,“Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression” IEEE Students’s Conference on Electrical, Electronics and Computer Science (SCEECS), 2016.