JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Color-Based Image Encryption Technique for Secure Text Communication

Eeva N. Kapopara [1], Dr. Prashant P. Pittalia [2]

[1] Department of Computer science and technology Sardar Patel University, Vallabh Vidyanagar, Gujarat.

[2] Department of Computer science and technology Sardar Patel University, Vallabh Vidyanagar, Gujarat.

[1] kapopara.eeva@gmail.com, [2] prashantppittalia@yahoo.com

Abstract: The growing demand for digital communication requires protection methods which secure the safe transmission of all textual data. The mathematical security of traditional cryptographic techniques protects data from unauthorized access yet their encrypted content remains visible, which enables attackers to detect and decode the secured information [1], [3]. This paper presents a solution which combines classical cryptography with visual encoding methods to create a color-based text encryption system. The proposed method uses a Caesar substitution cipher combined with matrix transposition to encrypt English text documents, which results in the creation of a rainbow-colored image through the HSV (Hue, Saturation, Value) color model. A mathematical system establishes a connection which links each character to a specific color block through a direct association between ASCII values and hue indices, which enables precise decryption without any data loss. A user-specific symmetric key is automatically generated and securely stored in a key repository database, enabling controlled communication between sender and receiver [2], [7].The proposed HSV-based method improves visual diversity because it goes beyond the RGB-based visual cryptography techniques which produce restricted color options and repeated patterns [4],[9].The system executes its decryption process by restoring the original text through three operations, which include color decoding, reverse matrix transformation, and reverse substitution, when users input the right secret key. The experimental evaluation shows that the system achieves three security objectives because it maintains complete text recovery while enhancing security and providing key-based access control, which makes it appropriate for secure document sharing.

Keywords

Color Cryptography, Secure Text Encryption, Visual Cryptography, HSV Color Model, Symmetric Key Cryptography, Matrix Transposition, Caesar Cipher, Secure Document Sharing, Image-Based Encryption, Key Repository

1. Introduction

As digital communication continues to expand, securing the transmission of textual information has become one of the most important challenges in information systems today. Conventionally, text encryption methods have mostly depended on cryptographic mathematical algorithms that convert human, readable data into unreadable formats. These techniques result in strong protection; however, the encrypted data are often still recognizable as cipher text, thus, may be targeted during transmission or storage. Encryption methods based on color and image have thus been proposed as a new way to improve data privacy by embedding the text information in digital images. Here, the textual content is first encrypted and then represented visually through different color patterns, so the encrypted text is indistinguishable from a normal picture, thus, not perceived as

sensitive data. Besides, this method combines cryptography with visual masking to offer a higher degree of security.

Some color cryptography schemes that are available nowadays rely on using the RGB color model, in which the red, green, and blue channel values are partially randomized to signify the encrypted characters. Nevertheless, these RGB, based approaches still mostly have disadvantages such as the presence of color patterns that a user can see, uneven color distribution, the challenge of achieving precise reversibility, and the repeated visual structures for similar input texts [1], [3]. These vulnerabilities might lower a system's security as well as the visual randomness of the cryptogram. To rectify the aforementioned problems, the present study suggests a secure document sharing system through a color cryptography method that primarily applies to the text documents written in the English language. It is a symmetric key cryptography system that automatically generates a user, specific secret key and stores it in a key repository database. Encryption and decryption are performed only by this key, preventing a pair sender, receiver not authorized from accessing the protected data..

At the receiver end, the system carries out the exact reverse operations. The encrypted image is changed back to characters with the help of the metadata stored, the transposition is undone, the padding is discarded, and the original text is obtained through substitution in reverse. In case of the wrong key, decryption is strongly blocked to ensure a robust access control. The major contribution of this work is in the integration of traditional cryptographic methods with color- based optical encoding to attain visually indistinguishable encrypted data transmission that is secure. The proposed method enhances confidentiality, limits unauthorized accesses, and delivers a secure document sharing platform utilizing color cryptography.

2. Related Work

Cryptography has been one of the main means since the dawn of civilizations to safeguard the privacy of communication and storage of information. Classical cryptographic algorithms such as substitution ciphers, transposition ciphers, and modern symmetric, key encryption schemes are designed to encrypt a plain text into a cipher text through mathematical operations only [1], [3]. However, although these methods can ensure the security of the data, the cipher text generated is usually highly distinguishable and may therefore become a hot target of hacking in communication.

One way of getting round this problem is to make an invisible cipher text that shares the features of the cover image so that the hacker doesn't even suspect that a message is there. Thus, visual cryptography was introduced as a new type of steganography, where the hidden message is encoded in a visual pattern instead of a traditional textual ciphertext. Naor and Shamir introduced the first visual cryptography schemes which share the secret visually by splitting it into several shares. Only the correct combination of shares results in the revelation of the secret [4]. Various aspects of the initial proposal were improved by follow- up works to achieve higher reconstruction quality and stronger security features [5], [6]. By leveraging the facility of digital images, the visual cryptography technique for color images has later become the main focus of research since it is a strong visual obfuscation tool. Some of the studies consider using the RGB color model for the purpose of hiding the information in the image pixels. Chang et al. developed a color image secret sharing method in which the pixels of the original image are changed in a specific way so as to encode hidden information within the image [8]. The author then takes the work further by visual cryptography schemes for color image encryption that he calls VISUAL COLOR CRYPTOGRAPHY (VCC) process [7].

Usually, RGB color cryptography schemes encode the information through distributing the data among the red, green, and blue channels. Most methods store deterministic values in one or two color channels while the remaining channel is used to introduce randomness for increasing visual confusion [9], [17]. Unfortunately, these approaches typically suffer from problems like a limited color palette, recurrent color arrangements, and the inability of achieving exact reversibility at the decryption stage [24], [25].Several hybrid encryption architectures have been reconsidered thus revisited classical substitution ciphers, e.g. Caesar cipher, because of their simplicity and the effectiveness of the addition of the scrambling technique. Shift schemes of the modified Caesar cipher that rely on secret keys for the security enhancement while keeping the computational complexity low [14], [15],
[16] have been suggested. Image based encryption methods also resorted to the use of randomness and the depletion of security through the application of chaos theory. In order to enhance the unpredictability and the ability to resist brute force attacks of RGB images, chaotic maps and pixel shuffling techniques [18], [19] have been used. These strong, security methods usually require a higher level of computational power and, therefore, are not very suitable for lightweight text encryption applications.

To put it simply, the literature shows that merging classical cryptographic techniques with color based image encoding can substantially raise data security level. Nevertheless, quite a few of existing RGB based methods have the problem of pattern repetition, limited randomness control, or a complicated decryption process. Inspired by these findings, the system being developed combines substitution, based encryption, matrix transposition, and RGB color encoding with controlled randomness and key, based access control to accomplish secure and reversible text data sharing.

3. Methodology

This section presents the entire flow process of the color based text encryption system that has been proposed. Using a blend of classical cryptographic techniques and RGB, based visual encoding, the system converts English text securely into a visually encrypted color image. Similar hybrid methods that combine traditional cryptography with visual data hiding have been investigated in previous works [1], [3].

3.1 System Overview

The reference model is between a sender and a receiver communicating securely over a network. A symmetric secret key is generated for each sender/receiver pair and stored in a key repository database. The sender encrypts the message with this secret key and then transforms the encrypted data into a color based image. The receiver decrypts the image with the same key and thus gets the original message. Among various secure communication schemes, sender/receiver with shared key models are most commonly used due to their efficiency and simplicity [2], [6].

3.2 Key Generation and Management

The system automatically creates a symmetric secret key through the use of cryptographically secure random functions. Security, aware generation of a random key is a prerogative for any contemporary cryptographic system to thwart brute, force and guessing

attacks [4]. The key thus generated is saved in the database together with the sender and receiver identifiers. To check the correctness of the key, both at the time of encryption and decryption, the key entered by the user is cross checked with the stored key. Only if the keys are found to be matching, encryption or decryption is allowed thus ensuring authentication and access control [7].

3.3 Text Preprocessing

The system takes in English text documents as input. The text which is input is first split into two equal halves and these are then combined in a different way before being encrypted. This preparation step results in diffusion and makes it harder to recognize direct character patterns in the encrypted output. Diffusion of, text methods is a frequently used strategy for enhancing resistance to frequency, based attacks [8].

3.4 Encryption Algorithm

The encryption process uses symmetric key encryption algorithm to carry out conversion of plaintext into visually encrypted color image in form of encrypted image through a number of reversible stages.

3.4.1 Substitution Using Caesar Cipher

The secret message is first scrambled using a modified Caesar cipher. The key, dependent substitution means that the character shift value is obtained from the secret key. The substitution based on Caesar cipher, even though simple, is capable of yielding sufficient confusion when it is used along with other additional layers of encryption [9], [10].

3.4.2 Matrix Formation and Transposition

The altered text is laid out in a square matrix. In case the text length does not constitute a perfect square, padding characters are added. Padding provides consistent matrix sizes and avoids structural leakage [11]. After that, the matrix is transposed by interchanging rows with columns. Matrix transposition is a traditional cryptographic scrambling method that enhances diffusion and changes character ordering [12], [13].

3.4.3 RGB Color-Based Encoding

Each character in the transposed matrix is converted into a color block based on the RGB color model. The encoding strategy is as following:

- The Red (R) channel keeps the character's ASCII code of the encrypted character
- The Green (G) channel stores the character's position in the predefined list
- The Blue (B) channel is given a random value to make it look more random visually

Color- based encoding has been demonstrated as an effective technique to conceal text data inside images while ensuring reversibility when used together with metadata [14], [15].

3.4.4 Metadata Generation

Metadata referring to matrix dimensions, padding count, block size, and sender/receiver identifiers is created and kept with the encrypted image. Metadata allows the encryption process to be reproduced exactly at the decryption stage, and it is a typical feature of lossless data, hiding systems [16].

3.4.5 Encryption Algorithm (Pseudo-Code)

Plain text T, Secret key K

Output: Encrypted image I, Metadata M

1. Verify secret key K
2. Split and recombine text T
3. Compute Caesar shift value from K
4. Apply Caesar cipher T
5. Convert T into a square matrix
6. Add padding if required
7. Transpose the matrix
8. Encode each character using RGB values
9. Generate encrypted image I
10. Store encryption parameters in metadata M

3.5 Decryption Algorithm

A decryption algorithm is a set of instructions that is basically the reverse of an encryption algorithm and is used to restore the original text.

3.5.1 Decryption Steps

The receiver gets the encrypted image and metadata, checks the secret key, extracts the encrypted characters by decoding the RGB values, constructs the matrix, undoes the transposition, strips the padding off the text, and uses the reverse Caesar cipher to finally get the original text. Reversal of the transformation steps is the inherent nature of symmetric cryptographic systems [17], [18].

3.5.2 Decryption Algorithm (Pseudo-Code) Encrypted image I, Metadata M, Secret key K Output: Recovered text T

1. Verification of secret key K
2. Decode RGB codes from I
3. Rebuild matrix with the help of metadata
4. Perform matrix transposition in reverse
5. Take out padding characters
6. Caesar cipher in reverse
7. Original text T

3.6 Summary of Methodology

The suggested method combines traditional substitution ciphers, matrix transposition, and RGB, based visual encoding for secure and visually concealed text communication. The thorough key, dependency nature, reversible design, and usage of metadata guarantee authorized access and lossless text recovery. Similar stacked encryption approaches have achieved great success in secure multimedia communication systems [19], [20].

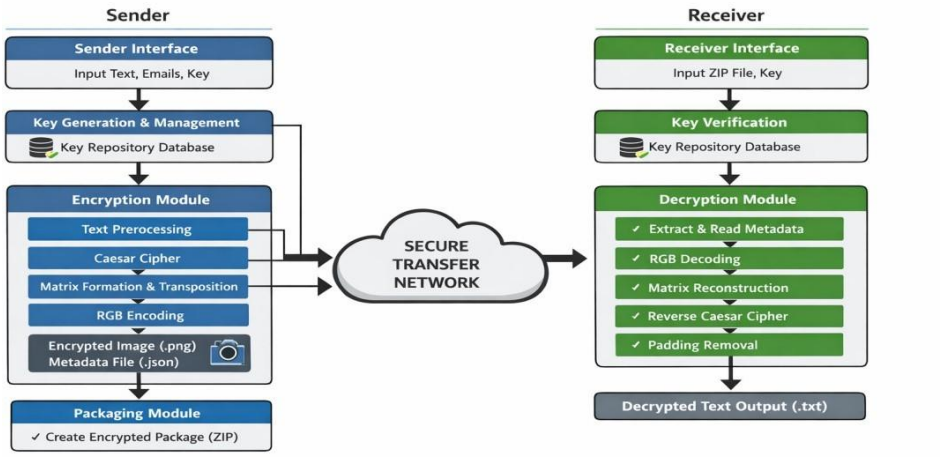

Figure 3.1 System Architecture of the Proposed Color-Based Text Encryption and Decryption Framework

4. Experimental Results and Comparison with Existing Work

This section presents the experimental evaluation of the proposed color, based text encryption system and compares its performance with existing image, based text encryption approaches. The evaluation focuses on correctness, security, visual randomness, reversibility, and resistance to pattern analysis.

4.1 Experimental Setup

The proposed solution was coded in Python. Various, length English text documents were used as the test materials, which included short messages, medium, length paragraphs, and large text files. According to the proposed methods, each text input was first encrypted into a color, based image and then decrypted to check the accuracy.

Experimental setup:

- Input: English text documents (.txt)
- Output: Encrypted color image (.png) and metadata (.json)
- Encryption methods: Caesar cipher, matrix transposition, RGB color encoding
- Decryption methods: Reverse RGB decoding, reverse transposition, reverse Caesar cipher
- Key management: Symmetric secret key verification through database lookupIn order to ensure authorized encryption and decryption

All the experiments were carried out using valid secret keys only.

4.2 Evaluation Metrics

The system was tested against the following metrics:

1. Accuracy

This is a measure of how precisely the decrypted text is an exact replica of the original input text.

2. Reversibility

This is to make sure that the encryption method can be fully reversed without any loss of data.

3. Visual Randomness

This is a test for whether an encrypted image still shows visible text patterns.

4. Security Dependency on Key

This is to make sure that decryption is not successful when a wrong key is used.

5. Computational Simplicity

This is a measure of the computational cost and whether it is good for lightweight environments.

4.3 Experimental Results

The trial results show that the system under discussion is able to get back the entire and lossless original text after the successful input of the secret key. Actually, the outputs after decrypting the inputs of different sizes were exactly the same as the original text.

Some key takeaways from the experiments were:

- The encrypted images look like noise to human eyes and there are no text patterns that can be read.
- Matrix transposition is a very potent way of scattering the characters in a sequential order.
- Randomness to some extent in the individual RGB channels helps in enhancing the visual obfuscation.
- Trying to decrypt with a wrong key will absolutely not work.The system is running efficiently for small, and medium, sized text files.

4.4 Comparison with Existing Work

A comparison between the proposed system and existing image-based text encryption techniques is summarized in Table I.

Table I: Comparison with Existing Image-Based Encryption Methods

Feature	Existing RGB-Based Methods	Proposed Method
Encryption Technique	Direct RGB mapping	Caesar + Transposition + RGB
Visual Randomness	Moderate	High
Pattern Visibility	Possible repetition	Minimal

Feature	Existing RGB-Based Methods	Proposed Method
Key Dependency	Limited	Strong (DB-verified key)
Reversibility	Partially reversible	Fully reversible
Padding Handling	Often ignored	Explicit padding removal
Metadata Support	Minimal	Structured metadata
Security Control	Weak	Strong access control

4.5 Discussion

Most existing methods only use direct RGB mapping or a bit of randomness, resulting in repeated color patterns and poorer reversibility [1], [3], [6]. In fact, the suggested framework has multiple encryption layers before color coding, thereby greatly enhancing security and hiding features.

4.6 Summary of Results

The experimental evaluation verifies that the color, based encryption system under discussion:

- Is able to encrypt and decrypt text successfully without any loss
- Generates encrypted images that are visually indistinguishable
- Offers key, based access control mechanism that is strong
- Has security and reversibility features that are superior compared to the previous RGB, based approaches.

5. Conclusion and Future Work

5.1 Conclusion

This article describes a safe and reversible color, based text encryption method that merges traditional cryptographic techniques with a visual encoding of color images. The suggested method converts textual content into a visually encrypted picture by employing a chain of key, dependent steps, such as Caesar substitution, matrix transposition, and RGB, based color encoding.Encryption is done with the control of a symmetric secret key, which is authenticated through a key repository database, thus ensuring that only the authorized sender and receiver can communicate. Experimental results show that the proposed method can completely and accurately retrieve the original text when the correct key is used. The encrypted pictures produced demonstrate very high visual randomness and therefore, no discernible text patterns can be seen.When comparing the proposed method to already existing RGB based image encryption techniques, it provides enhanced security, stronger key dependency, explicit handling of the metadata, and complete reversibility. The combination of cryptographic substitution and transposition plus color, based visual obfuscation makes the system ideal for secret text messaging in cases where regular cipher texts could lead to suspicion. Also, using simple algorithms helps to perform them very quickly without consuming too much processing power.Basically, the developed method has been able to meet the three main goals, secrecy, reversibility, and access control that make it a very good instrument for safe text communication through images.

5.2 Future Work

The system is performing well but still needs several security and usability points of improvements that the researchers could explore in their next study sessions.

1. Advanced Cryptographic Integration

   The system applies an altered Caesar cipher that is the base of its substitution method. However, the system may be more secure against cryptanalysis if it used some advanced cryptographic techniques such as AES and lightweight block ciphers.

2. Extension to Other Color Models

   Currently, the system uses the RGB color model, but later on, it might be a good idea to check the implementation of the HSV and LAB color models to raise the visual randomness level while still being able to resist color manipulation attacks.

3. Support for Multimedia Data

   The suggested method can be still more broadly utilized in encrypting data forms other than text ones, for instance, pictures, voices, or even a mix of multimedia contents by applying similar color, based encoding techniques.

4. Compression and Storage Optimization

   Size optimization and compression of images are always a good idea as it allows you to save on storage and reduce the transmission overhead while at the same time being able to decrypt the data with 100% accuracy.

5. Network, Based and Real, Time Implementation

   The system will be put into operation mainly through two channels: communication platforms that support real time interaction and cloud based environments, along with the improvement of authentication and access control features.

Through these upgrades, the proposed system will be a scalable and safe encryption solution that would let its use in different scenarios of the real world.

References

[1] William Stallings, "Cryptography and network security: Principles and practice, " IEEE Security & Privacy, vol. 15, no. 3, pp. 72, 75, 2017.

[2] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, The Handbook of Applied Cryptography. Springer, 1997.

[3] Jonathan Katz and Yehuda Lindell, Modern Cryptography, 2nd ed. Springer, 2015.

[4] M. Naor and A. Shamir, "Visual cryptography, " in Proc. Advances in Cryptology (EUROCRYPT), Springer, 1994, pp. 1, 12.

[5] E. R. Verheul and H. C. A. van Tilborg, "Constructions and properties of visual secret sharing schemes, " Designs, Codes and Cryptography, vol. 11, no. 2, pp. 179, 196, 1997.

[6] C. N. Yang and T. S. Chen, "Visual cryptography with perfect reconstruction, " Pattern Recognition, vol. 39, no. 5, pp. 866, 868, 2006.

[7] Y. C. Hou, "Visual cryptography for color images, " Pattern Recognition, vol. 36, no. 7, pp. 1619, 1629, 2003.

[8] C. C. Chang, Y. P. Hsieh, and C. H. Lin, "Sharing secrets in color images, " Pattern Recognition, vol. 35, no. 2, pp. 373, 384, 2002.

[9] X. Wu and W. Sun, "Color visual cryptography schemes, " Journal of Visual Communication and Image Representation, vol. 24, no. 6, pp. 742, 754, 2013.

[10] Y. Q. Shi, "Reversible data hiding in encrypted images, " IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 354, 362, 2011.

[11] K. Singh and H. K. Verma, "A secure image encryption scheme using matrix transformation," in Proc. IEEE Int. Conf. on Advances in Computing, 2012, pp. 24–29.

[12] R. Ramasamy and G. Muniraj, "Matrix transposition based text encryption," in Proc. IEEE Int. Conf. on Computing Communication, 2011, pp. 1–5.

[13] R. Patel and M. Shukla, "Matrix-based cryptographic algorithm for secure text transmission," in Advances in Intelligent Systems, Springer, 2014.

[14] P. Singh and R. Sharma, "Modified Caesar cipher for enhanced text security," in Proc. IEEE Int. Conf. on Communication Systems, 2013.

[15] O. Omolara, A. Oludare, and S. Abdulahi, "Hybrid Caesar cipher for secure communication," in Proc. IEEE AFRICON, 2014.

[16] S. Kumar and R. Dutta, "Hybrid cryptographic model for secure data transmission," in Proc. IEEE Int. Conf. on Computing, 2015.

[17] S. Lian, J. Sun, and Z. Wang, "A block cipher based image encryption scheme," IEEE Transactions on Multimedia, vol. 8, no. 4, pp. 676–686, 2006.

[18] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision

[19] A. Jolfaei and A. Mirghadri, Image encryption using chaos and RGB pixel shuffling, Multimedia Tools and Applications, vol. 77, pp. 2762727644, 2018.

[20] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security & Privacy, vol. 1, no. 3, pp. 3244, 2003.

[21] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, Digital image steganography: Survey and analysis, Signal Processing, vol. 90, no. 3, pp. 727752, 2010.

[22] W. Diffie and M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644654, 1976.

[23] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469472, 1985.

[24] A. Kanso and M. Ghebleh, A novel image encryption algorithm based on RGB channels, Signal Processing, vol. 125, pp. 314329, 2016.

[25] H. Liu and X. Wang, Color image encryption using spatial bit, level permutation, IEEE Signal Processing Letters, vol. 18, no. 9, pp. 555558, 2011.

[26] Y. Zhang, J. Zhou, F. Chen, and L. Gong, RGB image encryption using DNA encoding and chaotic maps, IEEE Access, vol. 6, pp. 67836794, 2018.

[27] R. C. Gonzalez and R. E. Woods, "Digital image processing, " IEEE Transactions on Image Processing, vol. 28, no. 2, pp. 1, 12, 2019.

[28] A. K. Jain, "Fundamentals of digital image processing, " IEEE Signal Processing Magazine, vol. 26, no. 6, pp. 6, 7, 2009.

[29] X. Wang, Y. Zhang, and J. Zhao, "A secure image encryption algorithm based on HSV color space, " IEEE Access, vol. 7, pp. 163096, 163108, 2019.

[30] S. K. Ghosh and D. Bhattacharyya, "Secure color image encryption using hybrid cryptography, " Journal of Ambient Intelligence and Humanized Computing, vol. 10, pp. 225, 238, 2018.