_____

A Hybrid Approach for Visual Cryptography Using Caesar Cipher Algorithm

[1]Aaditya Singh , [2]Akshay Jayant,[3]Rudransh Atray,[4]Aditya Pulkit, [5]Mr. Md. Shahid

[1,2,3,4,5]Computer Science & Engineering

Meerut Institute of Engineering & Technology

Meerut, Uttar Pradesh, India

Abstract: Protection and security of information against attacks is becoming crucial for individual people in today's world. New methods for safeguarding information from illegal intrusions are being developed by researchers at regular intervals. A number of cryptographic techniques have been identified, and much more is still to be uncovered. The purpose of the present paper is to examine a more advanced approach for hiding information known as visual encryption. Visual Cryptography is a unique encryption method that uses pictures to conceal information. Using the right image key, the encrypted image can be decrypted by the human eye. This cryptographic method can encrypt visual information, e.g. pictures and text, in a way that allows the person's visual system to decipher it if no computers are needed. A secret image is transformed into a series of shared images, which seem to be meaningful but noisy or distorted, as part of visual cryptography. The initial secret image can be revealed when the two shared images are merged.

This paper focuses on cryptography of black and white images and colored images using Caesar Cipher technique which is employed widely for entry level cryptographic techniques.

Keywords— Cryptography, Visual Cryptography, Image Encryption, Image Decryption, Caesar Cipher, Shift Cipher

1.   Introduction

The security of sensitive information is an essential element in today's technology. Image Encryption emerges as a vital solutionin this context, ensuring the confidentiality and integrity of visual data. This concept was first introduced in 1994 by Moni Naor & Adi Shamir [1] for the encryption of binary images. This prevents the visual message from unauthorized access and potential threats. There have been multiple advancements in the field of cryptography since then.
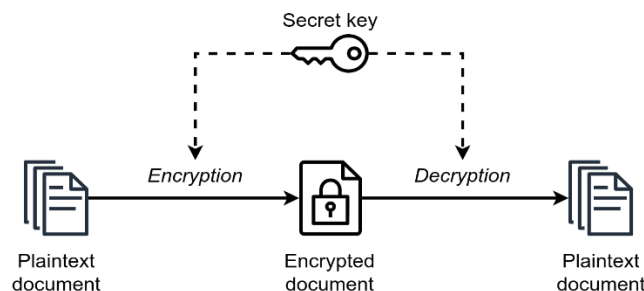

Fig.1(Symmetric Encryption)

_____

1.1   Components of Cryptography

The main components of cryptography [2] as are as follows:

- **Plaintext**: This is the original text or piece of information that needs to be encrypted.

- **Ciphertext**: This is the encrypted plaintext which has been converted to an unreadable format called ciphertext by the encryption algorithm.

- **Encryption**: This is the process which is used to encrypt the message into an unreadable format or ciphertext.

- **Decryption**: The Process of conversion of ciphertext back to its original form is called decryption.

- **Key**: This acts as an input to the encryption and decryption algorithms by which we can convert plain text into cipher text or convert it back into plain text.

1.2   Types of Cryptography

The traditional cryptography schemes usually deal with two types of encryption techniques: symmetric and asymmetric encryption [3]. Symmetric cryptography deals with a single key being used for the encryption process as well as for the decryption process (Fig.1) whereas in asymmetric cryptography scheme a public key is used to encrypt the image while for the decryption it requires a different key called "private key" as shown in (Fig.2). This ensures confidentiality of the message that only authorized people can decrypt the ciphertext.

Fig.2(Asymmetric Encryption)
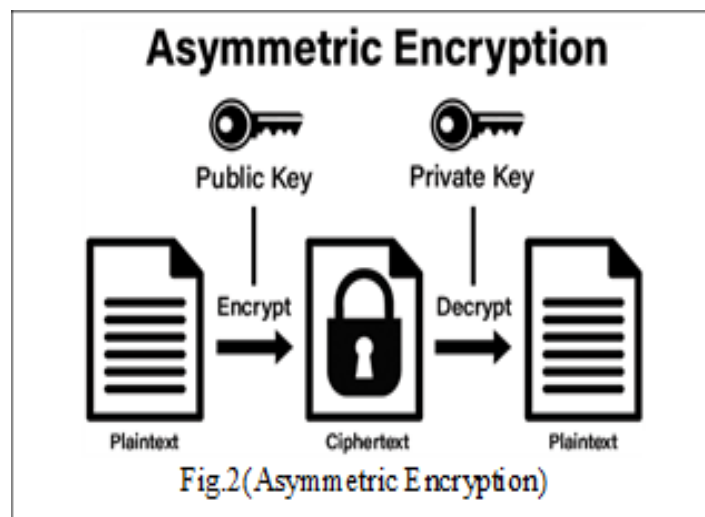
2. Caesar Cipher Algorithm

Caesar Cipher stands as one of the most fundamental and well-recognized encryption methods, also commonly referred to as the "Shift Cipher". Operating as a substitution cipher, it involves shifting each letter in the plaintext by a specific number of positions either forward or backward in the alphabet [4]. It is a type of **monoalphabetic substitution cipher**, meaning that each letter is replaced by another letter consistently throughout the entire message. For instance, with a key value of 3, each character in the plaintext is encrypted by shifting it three positions (Fig.3) in the alphabet to generate the ciphertext.

Fig.3(example of Caesar Cipher algorithm)
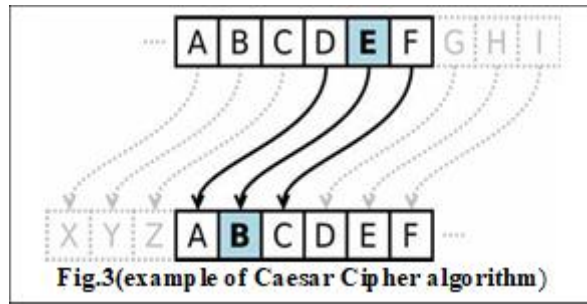
Here in this paper we will be using a new approach for image encryption by generation of random image mask

3. Related Work

[5] The Paper provides a thorough examination of image encryption techniques, encompassing chaos-based, spatial, frequency, and hybrid domain methods. Techniques highlighted include those utilizing chaotic maps, advanced encryption algorithms like AES, rotations, phase masks, Discrete Wavelet Transform (DWT), and S-box encryption. [6] The Paper Presents the significance of secure authentication in various sectors, emphasizing the importance of visual cryptographic protocols, particularly for images. It identifies challenges with conventional methods and introduces the optimized multi-tiered authentication protocol (OMTAP), integrated with visual sharing schemes, as a solution. OMTAP demonstrates robustness and broad applicability, ensuring image integrity and quality.[7] The combination of the Affine Cipher and RSA cryptography offers a potentially effective strategy for enhancing image security within the framework of Base64 encoding. This study emphasizes the necessity of utilizing advanced cryptographic methods to protect digital assets, reflecting the ongoing need for innovative solutions to address the evolving security landscape in the digital era.[8] This paper presents an innovative method in visual cryptography by employing a Hierarchical Visual Cryptography Scheme on gray images. The proposed scheme employs a fresh algorithm for producing gray shares, thereby amplifying the security of the original image via multi-level encryption.[9] This study presents a novel approach for color share generation using visual cryptography to bolster data security. The proposed method entails extracting R, G, and B components from a color image, applying a gray share generation algorithm exclusively to the R component, and amalgamating resulting gray shares with B and G components to produce color shares. During decryption, B and G components are extracted from all shares, and R gray shares are aggregated to unveil the secret image. The decrypted image preserves the original size and visual quality.[10] This research addresses banking security concerns arising from widespread internet usage and reliance on biometric authentication, proposing visual cryptography as a solution. By decomposing images into shares, the proposed (2, 2)-VCSXOR method ensures secure joint account transactions, mitigating identity theft risks.[11] this paper introduces a method for color image encryption in VC, generating two shares—random and key shares—without pixel expansion, reducing storage space. An enhanced encryption technique improves security and efficiency, with experimental results demonstrating superior encryption quality and reduced computation time.[12] The research explores visual cryptography's concept, aiming to encrypt a secret image into illogical shares that, when combined, unveil the original image without complex computations. Utilizing elliptic curve cryptography enhances privacy and security.[13] This research explores visual cryptography as a secure data transmission method by dividing digital images into printable transparent shares. Utilizing the human visual system, it ensures data security without complex computations. The proposed technique employs the Blowfish algorithm for encryption and decryption, implemented through MATLAB coding. Experimentation with various image formats and Blowfish algorithm adjustments reveals dynamic encrypted image histograms compared to originals. Notably, the method encrypts data efficiently on large 32-bit microprocessors and requires minimal memory usage. A test result for a sample image demonstrates its effectiveness.[14] The paper conducts a comprehensive review and analysis of existing VC schemes, noting advancements from single binary to color image sharing. While binary and grayscale images have yielded satisfactory results, color image schemes face challenges in contrast and resolution.[15] This paper

presents two constructions for threshold probabilistic Color-Black-and-White Visual Cryptography Schemes (PCBW-VCS) to address the pixel expansion issue. The constructions ensure non-expansible color shares and satisfy security and contrast conditions. In the first method, conventional VCS matrices are modified and transformed into PCBW-VCS matrices.

Fig.4 (Proposed Work Plan)
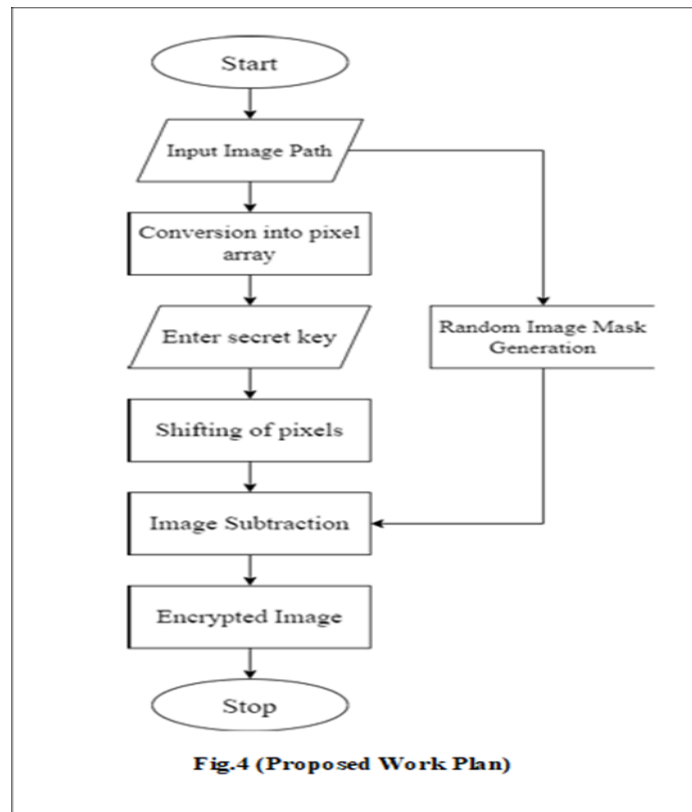
In the second method, PCBW-VCS distribution matrices are directly formed from conventional VCS matrices.[16] This work introduces two extended visual cryptography techniques for sharing color images. The first technique, (3, 3)-EVCT, generates three shares, each containing one color component of the secret image, while the second technique, (2, 3)-EVCT, requires any two out of three shares for reconstruction. Both techniques ensure meaningful shares to enhance security without loss of information. They are simple, efficient, and applicable to real-time systems, suitable for sharing images like medical and satellite imagery. Additionally, they can be extended for further security enhancement or sharing multiple secret images simultaneously.[17] This paper presents two enhanced visual cryptography schemes, (3, 3) and (2, 3), for securing image data. These schemes improve security and reliability compared to existing methods by utilizing keys and reducing computational overhead during decryption. The proposed encryption techniques ensure minimal pixel expansion and employ a shared key concept.[18] This paper introduces a new visual cryptographic scheme called (k, n)-VCS-tEC, which can correct errors in the shadow images that are created during the sharing process. This is important because in some situations, like the TiOSIS application, we need to make sure the shadow images are correct. Three different versions of this scheme are proposed, each with its own strengths and weaknesses. This approach ensures that even if there are mistakes in the shadow images, the original secret can still be recovered accurately.[19] This Paper introduces an innovative encryption method for 32-bit color images, utilizing four 1D chaotic maps to populate matrices representing color channels. Employing specific grids for channel encryption and utilizing the Four-square cipher method enhances security. The algorithm incorporates a right circular shift operation and applies the Arnold Cat Map transformation for added complexity. Rigorous security assessments demonstrate superior resistance to common attacks compared to existing methods, with a 25% to 44% increase in effectiveness. The novel encryption scheme effectively secures images, offering strong resistance against various

_____

attack types and ensuring high levels of security. This approach contributes significantly to the field of image encryption, providing a robust solution for safeguarding sensitive data.

Fig.5 Sample Image (RGB format)

4.   Design and Implementation

4.1   General Architecture

The architecture for the proposed idea is illustrated in the given image(Fig. 4) in the flowchart format. At the first user provides an image as an input. This image is then converted into an encrypted image by the encryption function. The encryption function shifts the values of the pixels accordingly thereby creating a new image.

This image is then converted into encrypted image by subtracting it from a masked image generated from the input image.

4.2   Module Description

4.2.1   Conversion into pixel array

The provided image is converted into a 2D matrix containing the pixel values of the image by using suitable modules available in any programming language.

Here we have converted a sample image having the RGB format (Fig.5) which is converted into the following pixel values:

[[[75 82 92]

 [74 81 91]

 [74 81 91]

 ...

 [102 111 120]

 [105 114 123]

 [105 114 123]]

[[74 81 91]

 [74 81 91]

 [73 80 90]

 ...

 [101 110 119]

[103 112 121]

[103 112 121]]

[[73 80 90]

[72 79 89]

[72 79 89]

...

[99 108 117]

[101 110 119]

[101 110 119]]

...

[[175 70 12]

[170 65   7]

[168 63   5]

...

[19 215 239]

[26 212 233]

[29 211 232]]

[[187 82 24]

[176 71 13]

[167 62   4]

...

 [6 202 226]

[45 230 251]

[49 228 248]]

[[196 91 33]

[180 75 17]

[165 60   2]

...

 [10 206 230]

[50 232 254]

[54 231 251]]]

4.2.2   Choosing a secret key

array by suitable methods. Then we select a shift value (key) for the pixels, all pixel values will be changed or shifted accordingly as per the selected key by the formula:

E(x)= (x+ key) mod n

4.2.3   Shifting of pixels

From the above stated formula where, E(x) is the encryption function which shifts the given value x, based on the provided key for the encryption which is summed up with the provided value of x then a mod function is applied to the summed value to provide the result within the given range of (0 to n-1). In the case of RGB pixels the value of n is 256. These encrypted pixel values are the converted back into an image when is now shifted.

Random Image Mask Generation

We generate random pixel values in (RGB format) which is of the same size and resolution as the input image provided in starting. We use randomly generated pixels in the range of (0 to 255) to create an image mask. This image mask is also saved in the device.
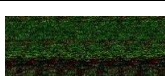
Image Subtraction
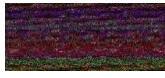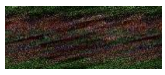
Now the generated shifted image from Caesar Cipher Algorithm and the randomly generated image mask having same resolution are opened in pixel values and both image matrices are subtracted from each other thus forming a new image matrix which is very hard to decrypt.

Final Encrypted Image

The image matrix obtained at the final step is then converted into an image thus obtaining the final encrypted image which is now meaningless and thus enhancing confidentiality and privacy.

5.   result analysis

For analysis of results, we have provided various different types of colored images to the algorithm and have received different types of output images which are listed below:

S. No.	Input Image	Output Image	Similarity Index	Output
1.			35.72	Meaningless
2.			35.54	Meaningless
3.			34.65	Meaningless
4.			36.07	Meaningless
5.			35.6	Meaningless
6.			32.1	Meaningless
7.			32.87	Meaningless

---

6. Conclusion

In the realm of secure communication, the paramount importance of safeguarding data serves as the driving force behind the exploration of a myriad of visual cryptography schemes. One particularly notable cryptographic innovation is Visual Cryptography (VC), specifically designed for the secure sharing of confidential images. The foundational principle of VC involves encoding an image into multiple shares, denoted as "n shares." These shares can manifest physically on transparencies or exist in a digital format.

Acknowledgment

References

[1] Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1994))

[2] Shobha Vatsa, Tanmeya Mohan, A. K. Vatsa: "Novel Cipher Technique Using Substitution Method" , International Journal of Information & Network Security (IJINS) Vol.1, No.4, October 2012

[3] D Paul Joseph, M Krishna, K Arun,"Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms", Volume 6, No. 3, May 2015 (Special Issue) International Journal of Advanced Research in Computer Science

[4] A. Rajan, D. Balakumaran, "Advancement in Caesar cipher by randomization and delta formation", ICICES, 2014.

[5] Hoshang Kolivand,Sabah Fadhel Hamood,Shiva Asadianfam,Mohd Shafry Rahim,"Image encryption techniques: A comprehensive review", in Multimedia Tools and Applications 2023.

[6] Tao Liu, Shubhangi Vairagar, Sushadevi Adagale, T. Karthick, Catherine Esther Karunya, John Blesswin A, and Selva Mary G, "Secure multimedia communication: advanced asymmetric key authentication with grayscale visual cryptography", in press http://www.aimspress.com/journal/MBE 2024.

[7] Andri Sukmaindrayana, Aneu Yulianeu, "Signature Security Development Utilizing Rivest Shamir Adleman and Affine Cipher Cryptographic Algorithms", IJISAE, 2023.

[8] Trupti Patel, Rohit Srivastava,"Hierarchical Visual Cryptography for Grayscale Image", in 2016 Online International Conference on Green Engineering and Technologies.

[9] Trupti Patel, Rohit Srivastava, "A New Technique for Color Share Generation using Visual Cryptography", IEEE,2016.

[10] Aaditya Jain, Sourabh Soni, "Visual Cryptography and Image Processing Based Approach for Secure Transactions in Banking Sector", 2017 2nd International Conference on Telecommunication and Networks.

[11] Al-Khalid, Randa A. Al-Dallah, Aseel M. Al-Anani, Raghad M. Barham, Salam I. Hajir, "A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes", Journal of Software Engineering and Applications, 2017, 10, 1-10.

[12] K. Shankar, P. Eswaran, "RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography", China Communications • February 2017.

[13] SM.Thamarai, Dr. T. Meyyappan, M.Karolin, "Encryption and Decryption of Color Images using Visual Cryptography", International Journal of Pure and Applied Mathematics.

_____

[14] Arup Kumar Chattopadhyay, Debalina Ghosh, Ram Sekher Pati, Amitava Nag, Sanchita Ghosh, "Visual Cryptography: Review and Analysis of Existing Methods", in The 6th Global Wireless Summit (GWS-2018).

[15] Xiaotian Wu, Ching-Nung Yang, "Probabilistic color visual cryptography schemes for black and white secret images", in X. Wu, C.-N. Yang / J. Vis. Commun. Image R. 70 2020.

[16] Kirti Dhiman, Singara Singh Kasana, "Extended visual cryptography techniques for true color images", in https://doi.org/10.1016/j.jvcir.2020.102793.

[17] Jyoti Tripathia, Anu Saini, Kishan, Nikhil, Shazad, "Enhanced Visual Cryptography: An Augmented Model for Image Security", Procedia Computer Science 167 (2020) 323–333.

[18] Ching-Nung Yang, IEEE Senior Member, Yi-Yun Yang, "On the Analysis and Design of Visual Cryptography with Error Correcting Capability" IEEE 2020.

[19] Mohammed Es-sabry, Nabil El Akkad, Lahbib Khrissi, Khalid Satori, Walid El-Shafai, Torki Altameem, Rajkumar Singh Rathore, "An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers" , Egyptian Informatics Journal 25 (2024) 100449   `   .