Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.778016

SHAMIR'S SECRET SHARING SCHEME USING VISUAL CRYPTOGRAPHY ON COLORED IMAGES

Geetanjali Agarwal
M. Tech Student, CTAE, Udaipur,

Dr. Kalpana Jain
Assistant Professor, CTAE, Udaipur
E-Mail-ID- geetanjaliagarwal17@gmail.com

Abstract –Nowadays, the risk of information dispersal during transmission through the communication channel has emerged as a real threat to the sender of the secret message, be it in the form of text or image. In the case of medical and military documents this is even more severe. To prevent this, an attempt has been proposed in the current research so that the problem can be solved efficiently and with ease and precision. The current research relies on the Shamir's algorithm. It tries to perform visual cryptography by the application of method like dividing the input image in a number of shares followed by shuffling each share and transmitting them. The reverse process is applied at the receiver end so that a majority of problem of data leakage can be controlled. The main focus is to encrypt colored images, a challenging task and needs real attention.Cryptography attacks are highly undesirable and hence a need arise to devise an algorithm which can prevent these attacks is required and the same has been attempted in the current research work. The NPCR and Entropy values were achieved 99% and 7.75 bits respectively which are ideal.
Keywords–Encryption, Decryption, Visual cryptography, Shamir's algorithm.

I. INTRODUCTION

Through cryptography which is a method of securing the transmission of confidential data via communication channel, sender of the message tries to safeguard the data with a high probability. The history of Cryptography focuses on the Egyptian reign, when Khnumhotep II's tomb from circa 1900 BC provide the first known samples of the usage of cryptography in some form.

The use of codes to secure information and communications in a way that only the intended recipients can decipher and process them is termed cryptography. Hence, information access by unauthorized parties is prevented. "Cryptography" is the combination of the words "crypt" (which means "hidden") and "graphy" (which means "writing").

Fields like military and health care are under the constant danger of cryptography attacks. To elaborate, cryptography attack means the stealing of sensitive information via the transmission channel. If not controlled in time, it can prove to be really dangerous and hazardous. Even a country's sensitive military documents may fall prey to the attacker's hands.

The two most common types of cryptography attacks are passive attack and active attack.

Passive Attack: As demonstrated by figure 1 [23], the passive attack gains unauthorized access to the confidential information and the sender does not even come to know that the data transmitted gets leaked in the process of communication because the information is not altered by the attacker and hence it is known as a passive attack.

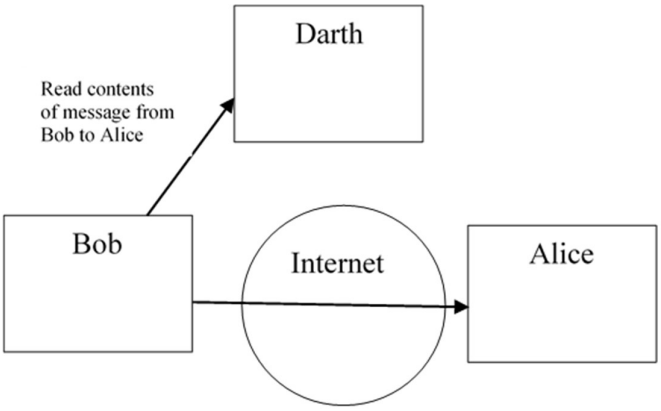

Fig 1: Passive Attack

Examples of passive attacks are Eavesdropping Wiretapping, Traffic analysis, Port scanning, Packet sniffing, Monitoring network traffic etc.

Active Attack:

Active attack means that there is a physical theft of things and the owner of the datacomes to know about the attack. This is because the data gets altered during attack process. This is demonstrated in the following figure 2 [23]

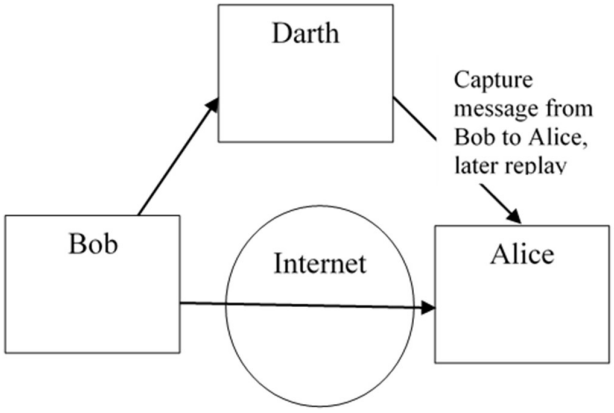

Fig 2: Active Attack

Examples of active attacks are Man-in-the-Middle, Denial-of-Service (DoS), Injection attacks, Malware infections, Phishing attacks etc.

Passive attacks are therefore more hazardous and an urgent need to prevent them arises.

The three types of cryptography are:

Secret key Cryptography: As the common key is used to both encrypt and decode the data, secret-key cryptography is also called symmetric cryptography as demonstrated by figure 3 [21]. Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and

RivestCipher 4 (RC4) are examples of well-known secret-key cryptographic algorithms.

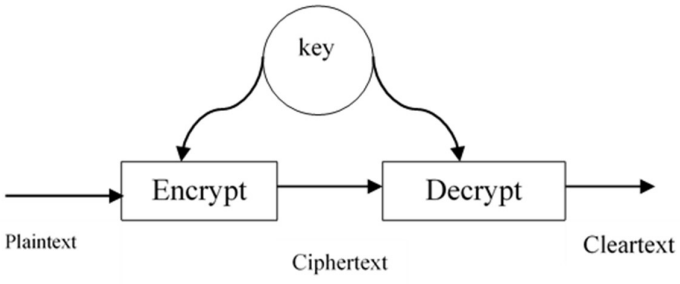

Fig 3: Secret key Cryptography

Public key Cryptography

A public key pair is used in public key cryptography and is associated with an entity that needs to digitally authenticate its identity or sign or encrypt material. Each private key is kept hidden while the corresponding public key is made public. This is as demonstrated by figure 4 [21].

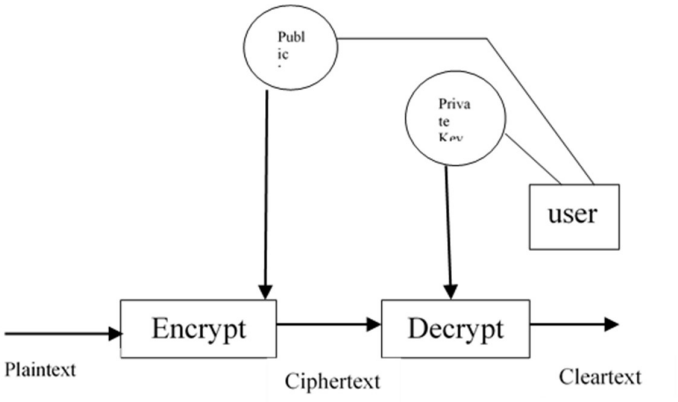

Fig 4: Cryptography using Public Key

Cryptography using Hash Function

As demonstrated by figure 5 [22],a hash function is a flexible one-way cryptographic technique that converts any size input into a distinct output with a predetermined number of bits. The result is a final unique identifier and is often referred to as a hash digest, hash value, or hash code.

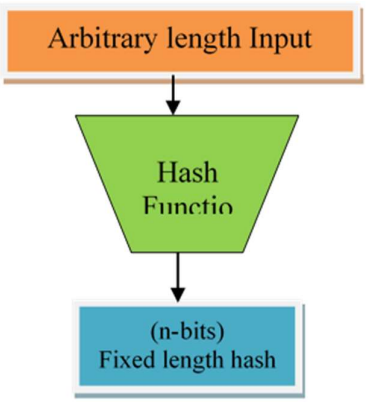

Fig 5: Hash Function Cryptography

An algorithm for distributing keys is called Shamir's Secret Sharing (SSS). The Rivest-Shamir-Adleman (RSA) algoristhm was co-invented by the well-known Israeli cryptographer Adi Shamir, after whom it is called.

A secret is split into pieces called shares by SSS. A group of participants in the discourse receive shares in the company. Shamir's Secret Sharing has the key property that the complete number of shares is not required to rebuild the secret rather; the pieces of the secret are combined to reconstruct the secret. The threshold is the amount that must be smaller than the total amount. In case just one or a few parties are absent, this helps prevent failures in the decryption of the sensitive information.

The present research tries to solve this issue using the already known Shamir's algorithm of Visual Cryptography which is resistant to computer attacks, as the shares are random and meaningless.

Visual Cryptography Applications

- It is a broad topic of study that is used for data concealment, picture security, color imaging, multimedia, and other related fields.
- It is used to hide data used in file formats, cybercrime, etc.
- It is used especiallyfor biometric security. Apart from this, it is also used in remote electronic voting and watermarking.
- It provides high quality realistic images and versatile applications, such as copyright protection, data integrity, and covert communication

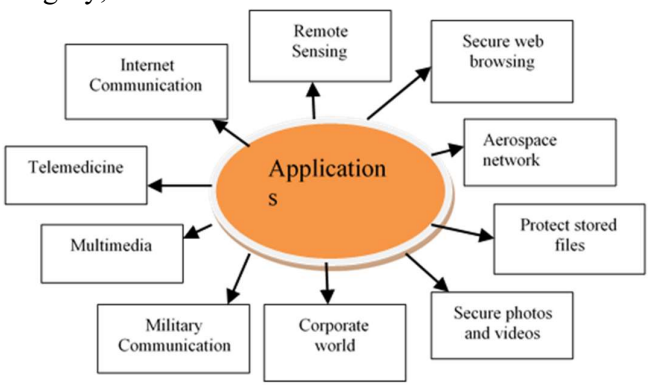

Fig 6: Applications of Visual Cryptography

The above figure 6 [24] shows the applications of Visual Cryptography

Advantages of Visual Cryptography

- Simple to use and comprehend.
- At the receiver side there are no complex calculations.
- No need for a secure channel to share the key.

- No specialized software is necessary.
- Resistance to computer attacks, as the shares are random and meaningless.

II LITERATURE REVIEW

[3] According to Anggraini, Dyah, and FarizanKazhimi, Shamir's secret sharing schemes are multiparty protocols. The transmission of digital images which are of the raster type frequently occurs in conjunction with the usage of internet for the exchange of data and electronic transactions.

The algorithm based on Shamir's scheme was used to encrypt a digital image (gray scale) with a resolution of 256x256 pixels to create a shared image with a resolution of 128x128 pixels and threshold values of (4, 8). The total number of shared photos was 8 parts, and at least 4 of those 8 parts were utilized in the recovery procedure.

Aninformation stored in digital image can be maintained private and secure since the outcome obtained by encrypting a grayscale image can provide an arbitrary shared image (i.e., no visible information).

[4] As per Benlashram, Arwa, recent years have seen a significant advancement in information and communication technologies, making it easier to share digital photographs on social media. However, since picture privacy is important in our society, maintaining image protection has become a significant barrier we must overcome. In this research, we suggest a brand-new picture encryption technique that makes use of a 3D chaotic map and image pixel shuffle. The 3D chaotic map is applied to the plain image after it has first been encoded via pixel shuffling, the output of which has then been XORed with a key.

[11] Reversible Absolute Moment Block Truncation Coding Visual Cryptography Scheme (RAVCS), developed recently by Yang et al., can hide a hidden image among n AMBTC shares. However, this process uses reference photos extensively. A PRAVCS using a single AMBTC reference image is introduced to decrease the number of reference images. As per the base matrices produced by the two suggested architectures, a binary secret picture is shared into n AMBTC shadow images during the encoding phase. By stacking enough bitmaps during the decoding phase, we can retrieve both the AMBTC reference picture and the secret image. Lossless reconstruction for the reference image is achieved when n AMBTC shares are used.

[12] According to Onuma, Kaito, and SumikoMiyatatherethere are more possibilities to transmit information online now as compared to previous time. Hence, there arises a need for a secure manner of doing so. Steganography, a communication tool that incorporates data into images, is garnering interest in this situation. The two basic types of image steganography are transform domain utilization and pixel value substitution. Most frequently, pixel value replacement steganography is applied, which makes use of the image's least significant bit (LSB). When secret information is contained in the lower bits of an image, it is, however, simple to predict. Here we suggest and analyze a correlation-

based steganography that embeds confidential data encrypted by Shamir's secret sharing scheme utilizing the spread spectrum approach.

[7] Gupta, KishorDatta, et almentioned in their paper that the quantum attack-resistant algorithm Shamir's Secret Sharing is extensively used in secret sharing. However, it can further be utilized in place of hashing in authentication systems. In this paper, we suggest an authentication protocol that will authenticate with the server using Shamir's secret sharing technique. In the post-quantum world, hashing could not be as effective in concealing data. Since hashing is a one-way encryption, in the post-quantum era, if any data servers are stolen, user credentials may also be at risk.

[2]Alapati, KalyanKoushik stated that effective access control strategies and protocols are needed to manage and secure company or government systems and data in the present highly distributed and hybrid-cloud environment. Currently, single-factor or multi-factor logins are often utilized throughout the business; however they are extremely vulnerable to hacking, phishing, and other password revealing techniques. Comprehensive data management and governance programs include group-oriented login or authorization procedures, where a group of people or processes (as opposed to a single person) provide their credentials/passwords or keys to access the sensitive resource. This is done to secure highly sensitive IT assets.
Secret Sharing, a well-known cryptographic method, provides an elegant and secure way to implement the group-oriented login. In this method, the secret (password) is divided into a certain number of shares, which are required in order to rebuild the secret (password). This cryptographic method is Shamir's Secret Sharing, whose splitting and reconstruction are based on polynomials over finite fields. The main aim s is to study and evaluate this technique with reference to threshold based group-login by various examples.

[15] Rahim, Robbi, and G. Suseendran (2020) presents a comprehensive literature review of secret sharingschemes presented by different researchers, its applications and the performance evaluation metrics.

[8] According to Kamble, Priyanka, and SonaliPatil everything is now readily available at home with the rise in internet usage. These developments cannot allow the medical industry to fall behind. But sharing medical colored images comes with several security dangers and threats. A medical organization's first duty is to ensure the security of patient records. This essay focuses on tamper-detection medical image security.

[1] A major area of security for digital data protection is the creation and application of appropriate fractal structures. By merging two one-dimensional fractals as seed functions from a wider range of fractal functions, this research suggests a generalized fusion fractal structure. Traditional Phoenix and Lambda fractals are combined to create a fusion fractal known as PLFF. The resulting PLFF fractal features improved randomized phase space, self-similar structure on different magnification scales, and fractional dimension. Its higher

complexity and wider chaotic range verify that PLFF can generate a pseudo-random number (PRN) sequence in both integer and binary forms. The resulting PRN sequences exhibit a high level of unpredictability and uncorrelation.
A new image encryption technique is proposed that uses a generated PRN sequence in the form of a secret key. It is established on the new PLFF fractal function. The working of the suggested encryption technique is examined using common security assessments such as histogram variance, NPCR and UACI tests for plain-image sensitivity, key sensitivity, information entropy, pixel correlation, noise and data loss, etc.

[5] As the information technology is increasing, the importance of security also has increased. The study of mathematical methods and associated information security concepts, such as data integrity, data confidentiality, and data authentication, is called cryptography. Visual cryptography (VC) encrypts a secret image into shares. This is a technique that prevents the leakage of the data in the original secret image. Its strength lies in the fact that the secret image can only be decrypted by humans and not computer technology.
Shamir and Naor suggested a fundamental paradigm by which natural images could be encrypted. This study presents a revolutionary VC approach for halftone images, where the produced image is represented in the size identical to the secret image. It is also suggested to conceal the visual information via pixel reversal and pseudo randomness.

[18] The method that separates the input image into a number of shares is called visual secret sharing. Every share contains some information, and the secret will become visible when k shares out of n stack up.
Less than k shares, however, do not function. The Human Visual System (HVS) was used for the process of decryption without the need for computing. We have put forth new methods for visual secret sharing (3, 3) and visual cryptography (2, 2). Our suggested strategies involve creating a gray scale image by stacking the shares, which yields an image of the size identical to the original secret image. In every strategy, we employed pixel reversal and randomization.

III OBJECTIVE OF THE RESEARCH

The main objective of the research work is to develop an efficient visual cryptography algorithm for the secure transmission of the digital images. The digital images especially the medical and military documents require a strong mechanism for securing the sensitive data during transmission over the communication channel.

The research work aims at developing a uniquemethod of encrypting image by splitting the image into a number of shares and then reconstructing the secret image at the decryption end. The focus of the research is to improve the way by which the Visual cryptography algorithm performs.

IV RESEARCH METHODOLOGY

The complete research process has been categorized as follows:

- ✓ Encryption
- ✓ Decryption

The dataset utilized in the current research work is taken from SIPI Image Dataset – MISC [https://sipi.usc.edu/database/database.php?volume=misc].
The images obtained from the dataset have been converted to png format.

Proposed Encryption:

The main goal of encrypting the image is to securely transmit it across the communication channel. This process is highly important because there is a good probability that the confidential image included in the original image could be leaked before it reaches its destination if it is not correctly encrypted.

Steps involved in Encryption process:

1. Extract the input image into its red, green and blue components.
2. Divide each of the components in to a number of divisions (let say n)
3. The resultant shares from the previous step are then shuffled using a shuffling algorithm into n shuffled shares.
4. Now the first share from all the three channels of these randomly shuffled shares will be combined to makethe share 1 and so on till share n.

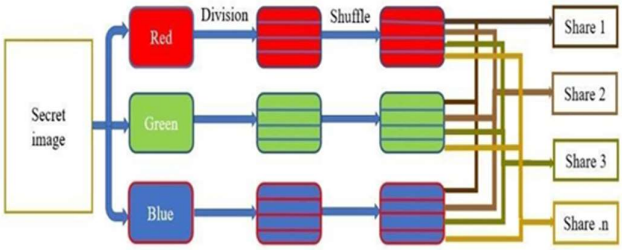

Fig7: Proposed Encryption process

Proposed Decryption:

The following steps describe the decryption process in brief:

1. Red, Green, and Blue channels are extractedfrom each individual share.
2. To obtain the shares, the shares previously obtained are deshuffled.
3. The red channel is now formed by combining all of the red shares of the deshuffled n-shares, and the same is true for the blue and green channels.
4. To create the input image, the red, green, and blue channels obtaisned above are merged.

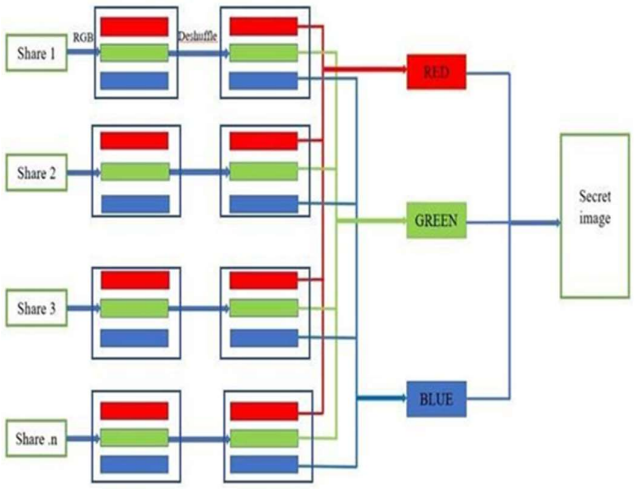

Fig 8:Proposed Decryption process

V EXPERIMENTAL RESULTS

In the current research work, results were evaluated and the two important metrics used were as follows:

Number Of pixel Change Rate (NPCR): It is not necessary that given two images with seemingly identical appearances have the same pixel intensities. The percentage of pixels that are different in the two encrypted images created by changing a single bit in the image is measured by the number of pixel change rate.

Mathematically, this can be stated as:

$$NPCR = \sum_{i,j} \frac{D(i,j)}{MN} X\ 100\% \quad \text{------1}$$

$$D(i,j) = \begin{cases} 0, if\ C1(i,j) = C2(i,j) \\ 1, if\ C1(i,j) \neq C2(i,j) \end{cases} \text{------2}$$

Where D (i,j) denotes the pixel value at (i,j) in original and output image. C1 is the original image and C2 is the cipher image. M x N gives the image size.

Entropy:

Entropy is a statistical measure of randomness utilized to characterize the texture of the secret image. In image, Entropy is defined as corresponding states of intensity level which individual pixels can adapt.

Mathematically,this can be stated as:

$$H(m) = -\sum_{i=0}^{N-1} P(m_i) log_2[P(m_i)]$$

Where N refers to the total number of pixel values, m_i indicates to symbol source and $P(m_i)$ refers to the probability of the symbol. H(m) is the entropy value.

The following table gives the comparison of NPCR value for n=7 and k=5

n,k = 7,5NPCR (%)		
IMAGE	REF. [15]	PROPOSED ALGO
LENNA	99.65	99.33
PEPPERS	99.66	99.29
MANDRILL	99.65	99.29
ALL IMAGES AVERAGE	99.65	99.30

Table 1: Table showing Comparison of NPCR value of the proposed algorithm with pixel shuffling and 3D chaotic map

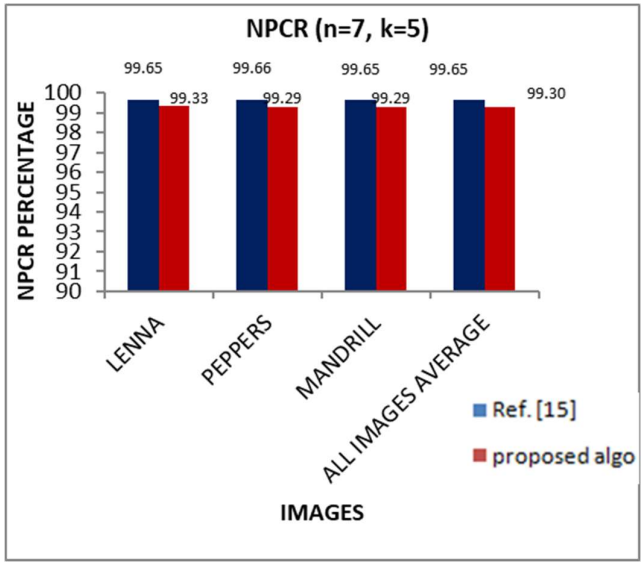

Fig 9: Performance comparison of NPCR of proposed algorithm with pixel shuffling and 3D chaotic map

The following table gives the comparison of entropy value for n=7 and k=5

n,k = 7,5 Entropy (bits)		
IMAGE	REF. [15]	PROPOSED ALGO
LENNA	7.99	7.75
PEPPERS	7.99	7.67
MANDRILL	7.99	7.75

ALL IMAGES AVERAGE	7.99	7.72

Table 2: Comparison of Entropy value of the proposed algorithm with pixel shuffling and 3D chaotic map

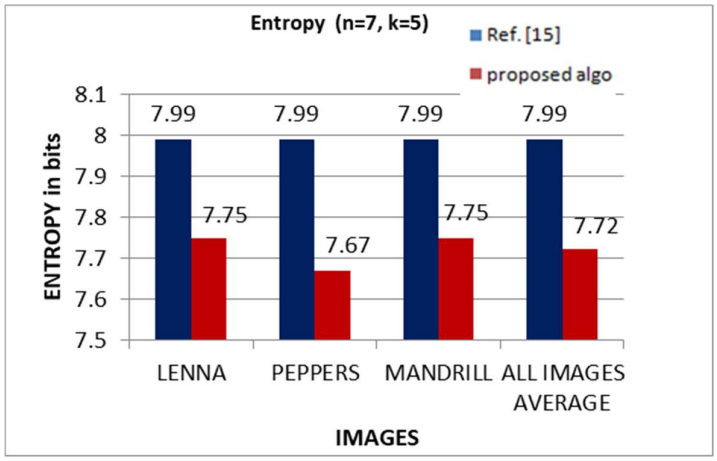

Fig 10: Performance comparison of Entropy of proposed algorithm with pixel shuffling and 3D chaotic map

Figure 9 and figure 10 show the comparison of the proprosed algorithm based methodology over 3 images.

VI CONCLUSION

Cryptography attack is a growing problem because attackers are constantly coming up with new techniques to steal sensitive information that is conveyed across communication channels. The study's major goal is to compare the visual cryptography algorithms that are already in use. It finds the one most efficient for facing cryptographic attacks. A good NPCR (Number of Pixels Change Rate) and Entropy are promised by the study. To get good results, we have adapted Shamir's technique for visual cryptography. The secret original image was encrypted using the division and shuffling technique, while the decryption end employed the opposite technique. The constantly evolving technological world is under constant danger from cryptography attacks. These attackers are in constant search of ways to steal private information, including crucial military documents or even medical records. Consequently, techniques like Shamir's algorithm, which encrypts the secret image before sending it, have been developed to stop these cryptography attacks, protecting users from being attacked along the route.

The current study shows how the Shamir's scheme can be utilized for image encryption for investigating this problem. The goal of the research was to develop an algorithm that can produce proper results. Python was used to construct this, and Google Colab, a very user-friendly and effective cloud-based coding tool, was used as the platform.

A satisfactory accuracy percentage was achieved. This is quite desirable. The method does not require any key for the encryption process. The division and shuffle technique worked well and was found efficient.

VII FUTURE SCOPE

It is expected that a visual cryptography method must have a minimal pixel expansion, strong security characteristics, improved contrast, and a straightforward algorithm.Traditional (k, n) visual cryptography is easy to implement but has a high pixel expansion.

Cloud-based visual cryptography is a unique method that offers complete reconstruction and increased security. It is crucial that the shares generated should be totally different and that a high-quality image is returned during the reconstruction of the secret so that the confidential data is preserved.

A lot of room for improvement in the realm of visual cryptography in terms of offering better secure algorithms that are also lightweight and easy to use exists.Additionally, it allows for the safe transmission of images with embedded data. Data is embedded using a variety of secure approaches, including data hiding in encrypted images and data hiding in scrambled images, among others. It is possible to research several aspects of visual cryptography algorithms and integrate them with the idea of the cloud to create a better safe algorithm that has no flaws. Hence, there is a lot of promise in the field of visual cryptography based on the concept of cloud.

A private block chain with permissions that is used to encrypt and safeguard the image exists. This approach ensures the confidentiality of the information in the image by storing the cryptographic pixel values of the image on the block chain.

REFERENCES

[1] Ahmad, Musheer, et al. "An image encryption algorithm based on new generalized fusion fractal structure." Information Sciences 592 (2022): 1-20.

[2] Alapati, KalyanKoushik. Group-oriented secret sharing using Shamir's algorithm.Diss. RutgersUniversity-Camden Graduate School, (2018).

[3]Anggraini, Dyah, and FarizanKazhimi. "Encryption OnGrayscale Image For Digital ImageConfidentiality Using Shamir Secret Sharing Scheme." Journal of Physics: Conference Series. Vol.710.No. 1.IOP Publishing, (2016).

[4] Benlashram, Arwa, et al. "A novel approach of image encryption using pixel shuffling and 3D chaoticmap." Journal of Physics: Conference Series. Vol. 1447.No. 1.IOP Publishing, 2020.

[5]C. R. Babu, M. Sridhar and B. R. Babu, "Information hiding in gray scale images using pseudo-randomized visual cryptography algorithm for visual information security," *2013 International Conference on Information Systems and Computer Networks*, Mathura, India, 2013, pp. 195-199, doi: 10.1109/ICISCON.2013.6524202.

[6]Ding, Hai-yang, et al. "A (k, n) Visual Cryptography Based on Shamir's Secret Sharing." Proceedings ofthe 3rd International Conference on Multimedia Systems and Signal Processing. 2018.

[7] Gupta, KishorDatta, et al. "Shamir's Secret Sharing for Authentication without ReconstructingPassword." 2020 10th Annual Computing and Communication Workshop and Conference(CCWC).IEEE, (2020).

[8]Kamble, Priyanka, and SonaliPatil. "Medical image security with cheater identification."2018 fourthinternational conference on computing communication control and automation (ICCUBEA).IEEE,2018.

[9]Kanso, Ali, and Mohammad Ghebleh. "An efficient lossless secret sharing scheme for medicalimages." Journal of Visual Communication and Image Representation 56 (2018): 245-255.

[10]Krishnan, Arun, and ManikLal Das. "Medical image security with cheater identification using secretsharing scheme." Proceedings of the International Conference on Signal, Networks, Computing,and Systems: ICSNCS 2016, Volume 1. Springer India, 2017.

[11]Li, Peng, Ching-Nung Yang, and Qian Kong. "A novel two-in-one image secret sharing scheme based onperfect black visual cryptography." Journal of Real-Time Image Processing 14 (2018): 41-50.

[12]Onuma, Kaito, and Sumiko Miyata. "AProposal for Correlation-Based Steganography Using Shamir'sSecret Sharing Scheme and DCT Domain."2021 International Conference on InformationNetworking (ICOIN).IEEE, (2021).

[13]Orłowski, Arkadiusz, and Leszek J. Chmielewski. "Generalized visual cryptography scheme withcompletely random shares."Proceedings of the 2nd International Conference on Applications ofIntelligent Systems. 2019.

[14]Orłowski, Arkadiusz, and Leszek J. Chmielewski. "Randomness of shares versus quality of secretreconstruction in black-and-white visual cryptography." Artificial Intelligence and Soft Computing:18th International Conference, ICAISC 2019, Zakopane, Poland, June 16–20, 2019, Proceedings,Part II 18. Springer International Publishing, 2019.

[15]Rahim, Robbi, and G. Suseendran. "VISUAL SECRET SHARING: A REVIEW." Journal of CriticalReviews 7.9 (2020).

[16]Shamir, Adi. "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

[17]Sudha, M. S., and T. C. Thanuja. "Randomly tampered image detection and self-recovery for a textdocument using Shamir secret sharing."2016 IEEE International Conference on Recent Trends inElectronics, Information & Communication Technology (RTEICT).IEEE, 2016.

[18]TalalMousaAlkharob,Aleem Khalid Alvi.et al. "New Algorithm For Halftone Image Visual Cryptography" IEEE 2004

[19]Wu, Xiaotian, and Ching-Nung Yang. "Probabilistic color visual cryptography schemes for black andwhite secret images." Journal of Visual Communication and Image Representation 70 (2020): 102793.

[20]Wu, Xiaotian, et al. "A (k, n) threshold partial reversible AMBTC-based visual cryptography using onereference image." Journal of Visual Communication and Image Representation 59 (2019): 550-562.

[21]Alvarez, Gonzalo & Li, Shujun. (2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems.. I. J. Bifurcation and Chaos. 16. 2129-2151. 10.1142/S0218127406015970.

[22]Amin, Md. Ratul & Zuhairi, Megat & Saadat,. (2020). A Survey of Smart Contracts: Security and Challenges. International Journal of Advanced Science and Technology. 9867-9878.

[23]R.Shrekhande, & Bairagi, Vinayak. (2010). "Lossless Medical Image Security",. Integrated Publishing Association International Journal Of Applied Engineering Research, Dindigul, ISSN 09764259,. 1. 1-4.

[24]Singh, Monu & Singh, Amit. (2022). A comprehensive survey on encryption techniques for digital images. Multimedia Tools and Applications. 82. 1-33. 10.1007/s11042-022-12791-6.