BLOCKCHAIN DATA PRIVACY SOLUTION BASED ON IPFS CRYPTOGRAPHIC PROTOCOLS

[1]ABDELAZIZ ELBAGHDADI, [2]ASMAA HILMI, [3]SOUFIANE MEZROUI, [4]AHMED EL OUALKADI[1,2] Abdelmalek Essaadi University, National school of applied sciences of Tangier, Laboratory of Information andCommunication Technologies (LabTIC) ENSA Tanger, Route Ziaten, BP 1818, Tanger principale, Morocco

[3]Soufiane Mezroui, Abdelmalek Essaadi University, National school of applied sciences of Tangier, Mathematics, and Intelligent Systems (MASI) ENSA Tanger, Route Ziaten, BP 1818, Tanger principale, Morocco
[4]Ahmed El Oualkadi, Abdelmalek Essaadi University,National School of Applied Sciences of Tetuan (ENSATe) , Laboratoire d'Ingénierie des Systèmes Innovants (ISI) ENSA Tétouan, BP: 2222 M'hannech II. Tétouan, Morocco

E-mail: [1]abdelaziz.elbaghdadi@outlook.fr, [2]asmaa00hilmi@gmail.com,
[3]mezroui.soufiane@yahoo.fr [4]aeloualkadi@uae.ac.ma,

ABSTRACT

To store the data in a decentralized and distributed way without third entity the block chain technology is used. The data in this technology is immutable and verifiable and its works without a third party. But blockchains faces of problems of scalability, security, and potential privacy, such as the ability to link transactions, the privacy of data on the blockchain or the conformity with privacy regulations. In this work, we propose an approach to share images with the help of blockchain, Interplanetary File System (IPFS) Protocol and visual cryptography. Furthermore, the proposed architecture aimed to solve the problem of image data privacy in distributed system. The proposed approach proceeds to encrypt and decrypt images using the RGB color decomposition principle (Red, Green, and Blue). Then the blockchain and IPFS protocol are used to ensure the data privacy in the distributed system. The simulation results of the proposed solution provide high security, and the security analysis including Peak Signal to Noise Ratio (PSNR), histogram analysis and correlation coefficient maintains a lossless encryption and reveals a high performance.

Keywords: *Blockchain, Cryptography, Security, Data Privacy, Confidentiality*

1. INTRODUCTION

Blockchain is coming in 2008 to create the first cryptocurrency. This technology is applied in general in the cryptocurrency and decentralized system. Furthermore, a set of protocols and consensus are used to solve the double spending problem which this technology makes all transaction available in public. The progress of the implementation of Blockchain opens a set of challenges and issues in this technology like anonymity, data privacy and Money Laundering [1][2]. The principle of visual secret sharing is decoding the secret image visually, by superimposing the shares [3]. Utilizing the Naor and Sahmir approach [4], a secret image into m shares can be encoded with the help of Visual cryptography Scheme (VCS), and m shares or more can be used to reconstruct and to reconstruct the secret image m shares or more can be used and other hand, we can’t have any information smaller to m. The shares are printed on a distinct transparency [5], when they are transmitted after applying encrypt and decrypt cryptographic techniques, superimposed them, the secret image should be visible. Ensuring a high level of security with lossless encryption is the most challenging of several research which has in VCS. In [6], the authors have extracted the Ri, Gi and Bi colors from the RGB image. Then, they create their shares by dividing every pixel’s value in Ri, Gi and Bi by 2. Once the shares are created, the Advanced Encryption Standard (AES) algorithm is used to both encrypt and decrypt them separately. The proposed method of Shankar K and Eswaran is applied to divide the image's shares into blocks once multiple shares are created using the RGB-extracted pixel values [7-8]. The Elliptical Curve Cryptography (ECC) method is used to encrypt the share blocks and to decrypt the encrypted blocks. Authors in [9], have suggested a method which aims to use n+1 cover images to encrypt n grayscale images. To reconstruct the n secret images, the Boolean XOR operation is used. In this paper, we have proposed to transmit K=2, …N multiple secret images via blockchain and InterPlanetary File System (IPFS) network. Firstly, we suggest a technique to encrypt and decrypt the K multiple images, which is based on the separation of each image in RGB colors components. It is important to note that our technique is based on XOR function. Secondly, the encrypted shares obtained are transmitted via blockchain and IPFS Protocol, which we use Ganache Ethereum blockchain and Infura API to get access to IPFS network. The proposed paper is structured as follows: the related works are giving in the section 2. The proposed methodology is given in section 3. Section 4 presents the results and discussion. Finally, section 5 concludes the paper.

2. RELATED WORKS

IPFS ((InterPlanetary File System) is a peer-to-peer protocol used to store and share data in a distributed system, this protocol allows nodes in peer-to-peer network to host and receive data. IPFS is a file distributed system that work without a third party. Its aim is to connect a set of computer equipment to the same file system. The main characteristic of IPFS protocol is sharing the content online through the devices of the nodes in the system. The content can be shared with any user of the system who has the hash [10]. A set of the decentralized application uses an IPFS protocol to store all the social data (video, text, images) due to the blockchain not being able to store this type of the data. Two problems that can appear when applying IPFS in decentralized application. The first is the privacy issue and over personal data and the second is the data availability issue: the privacy issue refers to accessing all users of the system to data. and the availability of data means that you should be persistent and permanent which the persistence is related to an object and a process which is still exist after the father event is powered off or he died. Due to the difficulty to add the policy to IPFS system and the data is available in the public. Furthermore, any user of the system has the hash of the content can access data [10]. In [11], among the requirements of implementing Decentralized applications is scalability and data privacy, they also highlighted the limitations of using IPFS. In [12], describe the set of the privacy issues and challenges that arise in the implementation of Blockchain architecture in the different fields. A set of solutions for data privacy in the blockchain is proposed. In [13] a technique called Secure multi-party computation which the aim of this method is to divide data between N parties using secret sharing. A cryptography method called the Zero-Knowledge, which is a method that help one party, the prover, to prove to another entity, the verifier, that a Proof of the truth of a given statement, without revealing any information other than the fact that the proof itself is correct [14]. The commitment scheme is a solution proposed by G. Brassard and al which is a scheme that gives the chance to one party to commit to a chosen value while keeping it hidden to others, with the ability to retrieve the committed value after [15]. The Homomorphic Hiding method is proposed by C. Gentry and al for sharing and performing operations on data without revealing the private values which is homomorphic encryption [16]. The Ring Signatures is proposed by D. Chaum and al in the case of a group of members with private and public keys, furthermore, which this type of digital signature performed by one of membership without knowing signed it [17]. In this work we propose a solution about the problem of the IFPS protocol called Data Privacy using cryptography visual which a layer of cryptography is added to encrypted image before are stored in the ipfs network and its address is sotred in the blockchain. We examined research on image encryption methods and blockchain uses, [18-19] proposed an images encryption method founded on the use of various chaotic systems. A strategy used in data storage and transmission is proposed in [20], This concept is dependent on diffraction imaging with wavelength multiplexing. They use a traditional optical phase cover for encryption, and a mixed state decomposition technique is used for decryption. In [21], they suggested an encryption technique for critical data images of industries 4.0 based on blockchain technology. The overview of the related works revealed many key features of blockchain. The first is reliability; The blockchain plays a crucial role in introducing the idea of smart contact and doing away with third parties. The second is transparency, with a copy of the entire chain stored on each blockchain node. which runs on smart algorithms. Finally, the most important feature is decentralization, Blockchain users are not dependent on any third parties, and he has full control over his property. There are numerous methods for image encryption currently available, but several privacy challenges arise in the applications in different areas. The blockchain offers a comprehensive solution for decentralized devices and has a very strong encryption mechanism, making it the ideal solution for confidentiality issues. A comparison of the current methods is given in table 1. According to this comparison, we proposed multiple images encryption which is based on separation of each image in RGB components and transmit it via blockchain and IPFS, we run more tests and compare our findings to previous research.

Table 1 Encryption solutions

References	*Year*	*Encryption quality*	*Technique*	*Decentralized*
[20]	*2019*	*Normal*	*Three-dimensional chaotic system*	*No*
[21]	*2019*	*Normal*	*Coupled logistic bernoulli map*	*No*
[22]	*2019*	*Normal*	*Orbit Perturbation*	*No*
[18]	*2020*	*Good*	*Blockchain*	*Yes*
Proposed	*-*	*Good*	*Visual cryptography and blockchain*	*Yes*

3. PROPOSED METHODOLOGY

Due to the problem of the data privacy this paper is coming to propose an approach to solve the problem in image sharing in IPFS. We propose our solution to secure the use of this data. To ensure this, we will encrypt the data images using our technique based in visual cryptography and store the hashed value images in IPFS. Figure 1 shows the proposed architecture. The user chooses multiples image data to transmit them via blockchain using IPFS protocol. Before transmitting them, we encrypt the images data using visual cryptography to ensure data privacy. The output images are decrypted, and we check the strength with a series of tests that are given in the results section.

3.1 Proposed Encryption Algorithm

The principle of using the visual cryptography method is encrypt the secret images before transmitting them via the IPFS network. In the first step, a solution based on the RGB decomposition technique is used. The pixels' values of each K images are separated as follows: R1, G1 and B1 color components are extracted from image1, R2, G2 and B2 color components are extracted from image2 …. and RK, GK and BK color components are extracted from image K, where K=2… N. These individual color components are images which are represented as matrices as illustrated by Equation (1), their sizes are the same as their original images.

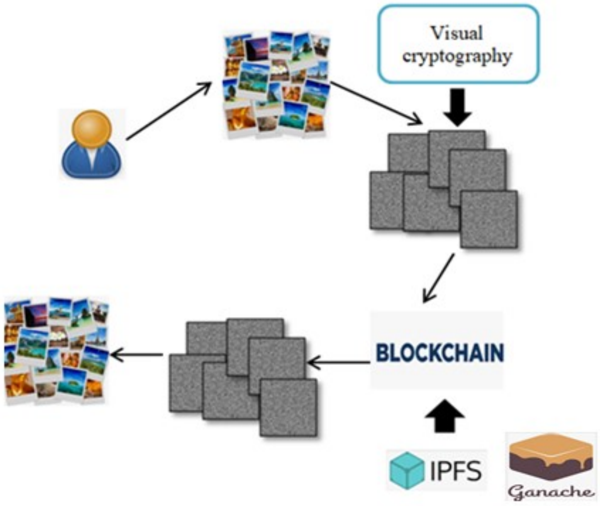


Figure 1: The Proposed Architecture

$$\begin{cases} image1 = (R1, G1, B1) \\ image2 = (R2, G2, B2) \\ \ldots \\ imageK = (RK, GK, BK) \end{cases} \tag{1}$$

Then, as shown by equation (2) every encrypted image is generated by applying an Exclusive-OR operation between color component of the secret image, other components from other secret images and a random key which is a matrix whose size is the same as that of the secret images. The encrypted images are denoted CRi, CGi and CBi with i=1...K, and the random key is denoted Km.

$$\begin{cases} CRi = Ri \oplus \sum_{i=1}^{K} G_{n-i} \oplus \sum_{i=1}^{K} B_{n-i} \oplus Km \\ CGi = \sum_{i=1}^{K} R_{n-i} \oplus Gi \oplus \sum_{i=1}^{K} B_{n-i} \oplus Km \\ CBi = \sum_{i=1}^{K} R_{n-i} \oplus \sum_{i=1}^{K} G_{n-i} \oplus Bi \oplus Km \end{cases} \tag{2}$$

To get the original images, the encrypted images are decrypted by using the Exclusive OR operation between them. Figure 2 summarizes the proposed solution starting from the secret images, through extracting color components from each image, then encrypting them until decrypting the encrypted images in order the reconstruct the initial images.

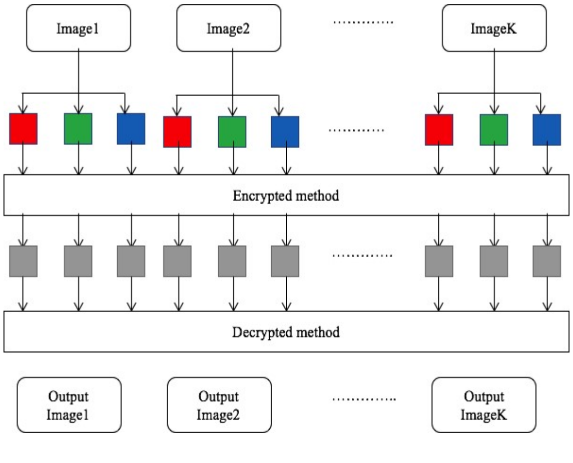
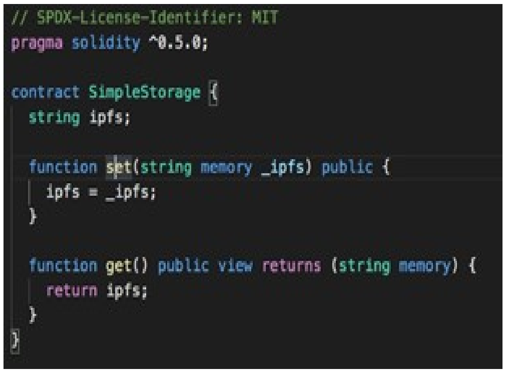


Figure 2: Block diagram of the proposed method

3.2 Transmission of encrypted images via blockchain

IPFS is a distributed peer-to-peer file system that does not need centralized servers. Its purpose is to connect a set of computer devices with the same file system. In the proposed architecture Infura's API networks are used to access IPFS networks. To store the IPFS hash in the blockchain, we use ganache blockchain and solidity language.



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.5.0;

contract SimpleStorage {
  string ipfs;

  function set(string memory _ipfs) public {
    ipfs = _ipfs;
  }

  function get() public view returns (string memory) {
    return ipfs;
  }
}
```

Figure 3: Smart contract in solidity

To access an image in the IPFS a hash address is used in figure 3 shows the smart contract to store this address in blockchain Ethereum using solidity.

4. RESULTS AND DISCUSSION

Three secret images have been chosen and tested to evaluate the performance of the suggested solution. First, we choose three RGB color images of the same size; Image1, Image2 and Image3. Next, every image is splitted into RGB components and each component is separately encrypted. Finally, the nine encrypted images are decrypted to retrieve the original image using our proposed technique. Equations (4), (5), (6) and Table.1 illustrate the performed processing. From equation (3), we extract the RGB colors for three images (image1, image2 and image3), then we apply the equation (2) to obtain the nine encrypted images (equation (4)).

$$\begin{cases} image1 = (R1, G1, B1) \\ image2 = (R2, G2, B2) \\ image3 = (R3, G3, B3) \end{cases} \quad (3)$$

$$\begin{cases} CR1 = R1 \oplus G2 \oplus G3 \oplus B2 \oplus B3 \oplus Km \\ CG1 = R2 \oplus R3 \oplus G1 \oplus B2 \oplus B3 \oplus Km \\ CB1 = R2 \oplus R3 \oplus G2 \oplus G3 \oplus B1 \oplus Km \\ CR2 = R2 \oplus G1 \oplus G3 \oplus B1 \oplus B3 \oplus Km \\ CG2 = R1 \oplus R3 \oplus G2 \oplus B2 \oplus B3 \oplus Km \\ CB2 = R1 \oplus R3 \oplus G1 \oplus G3 \oplus B2 \oplus Km \\ CR3 = R1 \oplus G1 \oplus G2 \oplus B1 \oplus B2 \oplus Km \\ CG3 = R1 \oplus R2 \oplus G3 \oplus B1 \oplus B2 \oplus Km \\ CB3 = R1 \oplus R2 \oplus G1 \oplus G2 \oplus B3 \oplus Km \end{cases} \quad (4)$$

$$Decrypted\_image_i = CRi \oplus CGi \oplus CBi \oplus Km \quad (5)$$

$$\begin{cases} Decrypted\_image_1 = CR1 \oplus CG1 \oplus CB1 \oplus Km \\ Decrypted\_image_2 = CR2 \oplus CG2 \oplus CB2 \oplus Km \\ Decrypted\_image_3 = CR3 \oplus CG3 \oplus CB3 \oplus Km \end{cases} \quad (6)$$

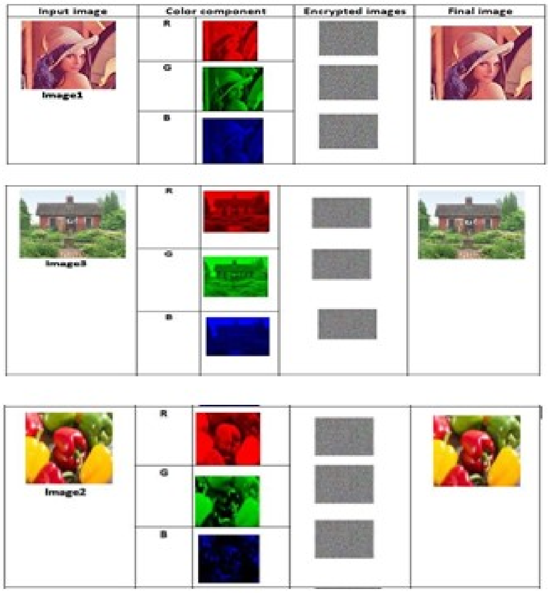


Figure 4: Secret images, RGB components, encrypted images, and final images.

4.1 The PSNR

The PSNR abbreviation mean The Peak Signal to Noise Ratio which is defined as the ratio between the maximum possible power of the signal and the power of the corrupted noise [23] and is provided by:

$$PSNR(dB) = 20\log_{10}\left(\frac{\max_i}{\sqrt{MSE}}\right) \quad (7)$$

Where maxi is the maximum possible pixel's value of the image, it is equal to 255. The pixels are represented using 8 bits per sample, and MSE is the Mean Squared Error which represents the average square of the error between the original and the reconstructed image. Theoretically, PSNR can be infinite if MSE equals 0, in this case there is no difference between the original and the reconstructed image, i.e., corresponding pixels of both images have similar values. The PSNR can also be calculated by [23].

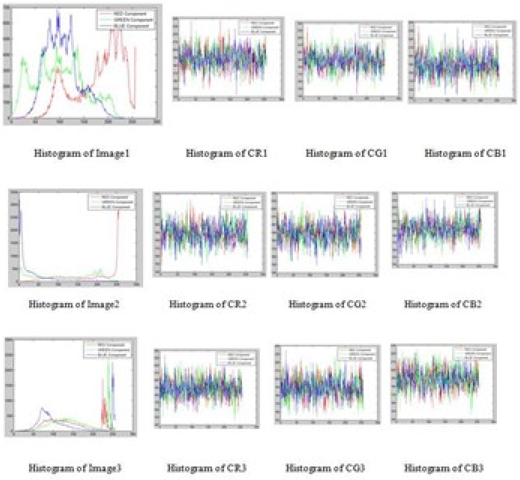
$$PSNR = \frac{1}{n}\left(PSNR(red) + PSNR(green) + PSNR(blue)\right) \quad (8)$$

Where, n is the number of all RGB color components. Table 2 shows the resulting PSNR and MSE values of every RGB component after decrypting the encrypted images of Image1, Image2 and Image3. For all used images (Image1, Image2 and Image3), the PSNR values of red, green, and blue components are infinite. The results and performance analysis show that the PSNR values are high and can achieve an infinite value due to MSE which equals to 0, this is means that corresponding pixels of original secret images and reconstruct image have similar values. Therefore, we conclude that our approach effectively hides the original hidden images and improves the quality of the rebuilt images.

Table 2 PSNR and MSE values between the original and final images (in dB)

4.2 Histogram analysis

The histograms illustrate the statistical characteristics of images. The histograms of secret and encrypted images are shown in Fig.5, it can see that the histogram after encryption process is the same that of the secret image for image 1, image 2 and image3, but before decryption, the encrypted images histograms are uniformly distributed, and they are significantly different significantly from that of the original images.



Histogram of Image1 Histogram of CR1 Histogram of CG1 Histogram of CB1

Histogram of Image2 Histogram of CR2 Histogram of CG2 Histogram of CB2

Histogram of Image3 Histogram of CR3 Histogram of CG3 Histogram of CB3

Figure 4: Histograms of both original images and encrypted images.

4.3 Correlation coefficient factor

The similarity between the original images and the encrypted ones can be better understood thanks to this study. The following equations can be used to describe how the neighboring pixel correlation coefficient factor functions [24].

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{9}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{10}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2 \tag{11}$$

Images	*MSE*	*PSNR (dB)*
Image1	*MSE(Red)=0* *MSE(Green)=0* *MSE(Blue)=0*	*PSNR(Red)=inf* *PSNR(Green)=inf* *PSNR(Blue)=inf*
Image2	*MSE(Red)=0* *MSE(Green)=0* *MSE(Blue)=0*	*PSNR(Red)=inf* *PSNR(Green)=inf* *PSNR(Blue)=inf*
Image3	*MSE(Red)=0* *MSE(Green)=0* *MSE(Blue)=0*	*PSNR(Red)=inf* *PSNR(Green)=inf* *PSNR(Blue)=inf*

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{12}$$

In which x and y represent the values of two neighboring pixels in the original or encrypted images, E(x) is the mean value of x, D(x) is the variance with respect to mean, cov (x, y) signifies the estimation of the covariance among adjacent pixels x and y, and rxy is the correlation coefficient between x and y. The correlation coefficient should be very low or near to zero for a better encrypted image. The calculated correlation coefficients for the initial and final images are presented in Table 3. From these results, it is noted that while the correlation coefficients for the encrypted images are nearly zero, the two neighboring pixels in the original images have a strong correlation to one another.

Table 3. Results of correlation values applied on both original and encrypted images.

4.4 Entropy analysis

The entropy, which Claude Shannon initially developed in [24], is an important test for examining the randomness of information and is used to evaluate the quality of image encryption. It can be calculated using Equation (13)

$$H(X) = -\sum_{i=1}^{n} \Pr(x_i)\log_2 \Pr(x_i) \qquad (13)$$

Where, X is the test random variable, xi is the ith possible value of X, and Pr (xi) is the probability of X = xi. An ideal encrypted image is one in which the pixel values are uniformly distributed throughout. If an encrypted image is very random-like, it is thought that its information entropy is very close to the theoretical maximum. Table 4 shows the entropy of encrypted images, which is very close to 8, the theoretical upper bound of entropy for an 8-bit image.

Table 4. Entropy values of encrypted images

Encrypted images	*Entropy*
CR1	*7.9988*
CG1	*7.9987*
CB1	*7.9991*
CR2	*7.9988*
CG2	*7.9986*
CB2	*7.9987*
CR3	*7.9989*
CG3	*7.9987*
CB3	*7.9988*

The aim of the proposed approach is to share the image data in the distributed system and ensure the confidentiality of the image which the user can store the encrypted data in the IPFS network and blockchain the Table 5 shows the feature of the proposed architecture.

images	*CORRELATION*		
	Horizontal	*Vertical*	*Diagonal*
image1	*0.9440*	*0.9727*	*0.9249*
CR1	*0.0001*	*0.0010*	*-0.0008*
CG1	*-0.0022*	*0.0010*	*-0.0007*
CB1	*-0.0012*	*0.0002*	*0.0017*
Image2	*0.9812*	*0.9921*	*0.9762*
CR2	*-0.0006*	*0.0005*	*0.0032*
CG2	*0.0019*	*-0.0018*	*0.0044*
CB2	*0.0015*	*-0.0012*	*-0.0025*
Image3	*0.9365*	*0.9275*	*0.8935*
CR1	*-0.0034*	*-0.0011*	*-0.0013*
CG1	*-0.0001*	*0.0017*	*-0.0004*
CB1	*-0.0019*	*0.0014*	*-0.0019*

Table 5: The Features Of Proposed Architecture

Cryptographic scheme	*Trusted Third Party*	*Data privacy*
Cryptography Visual	*Use the third party to ensure the privacy of the data.*	*Yes*

5. CONCLUSION

This paper proposes to use visual cryptography to transmit multiple secret images via IPFS network and blockchain to solve the problem of the image data privacy in distributed system. We start by dividing every secret image into three RGB color components, then we encrypt them separately. The IPFS network is used to share the encrypted image and the blockchain is used to store the IPFS hash. Finally, we decrypt the encrypted images to recover the secret image. The encryption and decryption processing are performed using our suggested techniques. Besides, our proposed encryption technique can encrypt N secret images, the results, and the performance analysis show that the proposed approach has many other advantages. In one hand, by using the visual cryptography to handle the secret images, we increase the level of security to transmit the reliable secret information. In other hand, when we receive the encrypted images, if some encrypted images are lost, it is impossible to retrieve the secret image. Also, the reconstructed images have high PSNR values which mean that they are of very high quality. Finally, our solution can hide efficiently the original secret images and increase the quality of the final reconstructed images. As mentioned previously the data privacy is one of the critical aspects and major challenges in the Blockchain Technology in the previous in the future work we will target the data analysis to detect the frauds in the Blockchain. As mentioned previously the data privacy is one of the critical aspects and major challenges in the Blockchain Technology in the previous in the future work we will target the data analysis to detect the frauds in the Blockchain. As mentioned previously, the data privacy is one of the critical aspects and major challenges in the Blockchain Technology in the previous in the future work we will target the data analysis to detect the frauds in the Blockchain.

REFERENCES

[1] F. Reid et M. Harrigan, “An Analysis of Anonymity in the Bitcoin System “, in Security and Privacy in Social Networks, Springer, 2013, p. 197-223.

[2] Abdelaziz El Baghdadi and al “SVM: An Approach to Detect Illicit Transaction in the Bitcoin Network” 2022, Springer

[3] A. Hilmi, S. Mezroui, &A. El Oualkadi “Overview of Visual Cryptographic Systems Based on XOR Function”, International Conference on Multimedia Computing and Systems (ICMCS), 2018.

[4] M. Naor and A. Shamir. “Visual cryptography. EUROCRYPT: Workshop on the Theory and Application of Cryptographic Techniques”, Italy, 1994, Springer

[5] W.Q. Yan and D. Jin and M. S. Kankanhalli “Visual cryptography for print and scan applications”. IEEE International Symposium on Circuits and Systems, Vancouver, 2004.

[6] F.Liu and C.Wu and X.Lin “ A new definition of the contrast of visual cryptography scheme. Information Processing”,2009.

[7] K. Shankar and P. Eswaran “RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique. Journal of Circuits, Systems, and Computers”, 25:1-23, 2016.

[8] K. Shankar and P. Eswaran. “RGB Based multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography. China Communications”,14:118-130, 2017.

[9] V. J. Kapadiya and L. S. Desai and Y. K. Meghrajani. “Boolean-based Multi Secret Sharing Scheme using Meaningful Shares”. Proceedings of the 2nd InternationalConference on Inventiv Communication and Computational Technologies, 2018.

[10] B. Guidi, A. Michienzi and L. Ricci, "Data Persistence in Decentralized Social Applications: The IPFS approach," 2021 IEEE 18th Annual Consumer

Communications & Networking Conference (CCNC), 2021,

[11] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez- Ramos, R. Torres Moreno, et A. Skarmeta, "Privacy- Preserving Solutions for Blockchain: Review and Challenges", IEEE Access, 2019,

[12] Archana Prashanth Joshi, Meng Han, Yan Wang, "A survey on security and privacy issues of blockchain technology". Mathematical Foundations of Computing, 2018,

[13] J. Pieprzyk, T. Hardjono, et J. Seberry, "Fundamentals of computer security. Springer Science & Business Media, 2013.

[14] R. Cramer et I. B. Damgård, Secure multiparty computation. Cambridge University Press, 2015.

[15] G. Brassard, D. Chaum, et C. Crépeau, "Minimum disclosure proofs of knowledge", J. Comput. Syst. Sci., vol. 37, no 2, p. 156-189, 1988.

[16] C. Gentry, ''Fully homomorphic encryption using ideal lattices,'' in Proc. 41st Annu. ACM Symp. Theory Compute. (STOC), New York, NY, USA, 2009,

[17] D. Chaum and E. van Heyst, ''Group signatures,'' in Proc. Workshop Theory Appl. Cryptograph. Techn. Springer, 1991, pp. 257–265.

[18] Li, H.; Wang, Y.; Zuo, Z. "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms" Opt. Lasers Eng. 2019

[19] C.E. Shannon. "A mathematical theory of communication", Bell System Technical Journal, 27:379-423 and 623-656, 1948

[20] Xie, Y.; Yu, J.; Guo, S.; Ding, Q.; Wang, E. "Image Encryption Scheme with Compressed Sensing Based on New Three-Dimensional Chaotic System". Entropy 2019

[21] Zhang, W.; Zhu, Z.; Yu, H. "A Symmetric Image Encryption Algorithm Based on a Coupled Logistic–Bernoulli Map and Cellular Automata Diffusion Strategy". Entropy 2019, 21, 504.

[22] Li, H.; Wang, Y.; Zuo, Z. "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms" Opt. Lasers Eng. 2019

[23] A. T. Nasrabadi, M. A. Shirsavar, A. Ebrahimi etM. Ghanbari, "Investigating the PSNR calculation methods for video sequences with source and channel distortions", 2014 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, IEEE, juin 2014.

[24] Sura F. Yousif. Grayscale, "Image Confusion and Diffusion Based on Multiple Chaotic Maps". 1st International Scientific Conference of Engineering Sciences - 3rd Scientific Conference of Engineering Science (ISCES),2018.