A New Approach to Ensure the Confidentiality of Data in Cloud Storage Environments

Abdullah Jaafar[#1], Abdul-Gabbar Tarish Al-Tamimi[*2]

[#]Computer Science Department, Faculty of Computers and Information Technology (Turba Branch), Taiz University
[*]Computer Science Department, Faculty of Applied Sciences, Taiz University
[1,2]Taiz, Yemen

***Abstract*— Cloud computing is a technology which supplies users multiple services and abilities such as storing their data in the cloud storage and manipulating it when needed. However, the data users are worried about the confidentiality of their data stored in cloud storage because the full control of users data is transferred to cloud storage providers. Therefore, to ensure the confidentiality of user's data in cloud storage, a security mechanism such as cryptography has to be provided to the data and it prefers to be simple, user-friendly and not complex. Visual cryptography (VC), also known as visual secret sharing (VSS), is a cryptographic technique for images that does not require any key management technique and does not need complex computations. For decoding, VSS schemes use visual inspection or the equivalence of simple OR Boolean operation on the shadow images which causes the contrast level to be lowered. In order to allow for lossless decryption, Wang et al. introduced a non-visual XOR-based secret sharing scheme without any loss in contrast. The main objective of this paper is to ensure data access in cloud storage by only authorized users. We propose a new approach to ensure the confidentiality of data in cloud storage environments by using XOR Boolean operation and XOR-based Wang et al.'s (n, n) secret sharing scheme. The resultant outputs of our encryption algorithm are meaningful shadow images by using public cover images. Therefore, each one of meaningful shadow images stored in different cloud server does not attract the attention of the inside malicious attackers and also it cannot individually recover the secret image.**

***Keywords*— Cloud, Data Confidentiality, Visual Cryptography, Secret Sharing, XOR Operation, Meaningful Shadow Images.**

I. INTRODUCTION

Cloud computing is a type of Internet based computing which means storing and accessing data and software over the Internet instead of PC's hard drivers. Cloud computing provides shared processing data, software and resources to its user when required. As user's data is stored in the cloud, the cloud provider has full control on the user's data but the data user (owner) has no control over his/her data. This makes the user's mind to thing about the security of the data in the cloud. The security is the major problem to cloud computing services [1-10]. Cryptography is one of the trusted practical methods for performing data security. The main purpose of the cryptography is to provide data confidentiality by converting the sensitive private data (known as plaintext) into unreadable and useless form (known as ciphertext) [10]. Confidentiality parameter is used to protect the data from insiders and outsiders attacks and therefore it ensures that only authorized users can be accessed to the data [1-10]. In 1994, Naor and Shamir [11] proposed a visual cryptography (VC) which is a special type of cryptography for images. It is also called a visual secret sharing (VSS) that is used to divide a secret image into n meaningless and non-identical shadow images (printed on transparencies) and distributes those shadow images to n participants. The reconstruction secret image in VSS schemes cannot be recovered with any one shadow image but it needs only the very simple Boolean 'OR' operation computation on the shadow images which is done automatically by the human eye when any k or more of these shadow images (where $k \leq n$) are stacked together, while in the classical cryptographic systems, complex computer operations are required, comparatively [12-16]. The drawback of the traditional VSS schemes, is the size of each shadow image, which expands the secret image size many times, thereby causing many problems such as image distortion, use of more memory space and difficulty in carrying shares [17]. To overcome the problems resulting from the pixel expansion, Ito et al. [18] and Yang [19] proposed the probabilistic visual secret sharing (ProbVSS) model for binary (black-and-white) images, without pixel expansion. They merged the concept of probability with the traditional visual secret sharing, to encode a black-and-white secret image into the same sized shadow images, as the secret image. As the result, the recovered image has the same size as the secret image. Table 1 shows the encryption and decryption processes of (2, 2) probabilistic secret sharing (ProbVSS) scheme with no pixel expansion, where a pixel on a black-and-white secret image is mapped into a corresponding pixel in each of the two shadow images. The original secret image is recovered by stacking and aligning carefully the pixels of the two transparent shadow images. This stacking process is computationally performed through the binary OR operation which causes the contrast level to be lowered. Generally, all or most the traditional VSS and the ProbVSS schemes have the contrast problem which produces a poor visual quality image during decoding (stacking) process [20-32]. In order to allow for lossless decryption, Wang et al. [32] proposed the (n, n) secret sharing scheme based on XOR operation. They have been shown that the original secret image can be recovered without any loss in contrast by simply substituting the OR operation as used in the traditional VSS and the ProbVSS schemes with the XOR operation, although the XOR operation needs extra computation. The XOR-based Wang et al.'s (n, n) secret sharing scheme produces an exact visual quality image during decoding without any loss in contrast. This scheme is not a "visual" scheme and cannot be implemented by directly the stacked transparencies of the shadow images because it does not use the OR Boolean operation. Table 1 shows also encryption and decryption processes of XOR-based Wang et al.'s (2, 2) secret sharing scheme, where a pixel on a black-and-white secret image is mapped into a corresponding pixel in each of the two shadow images. The original secret image is recovered by XORing the pixels of the two shadow images at the same positions. The proposed method in this paper uses XOR operation and XOR-based Wang et al.'s (n, n) secret sharing scheme to ensure the confidentiality of user data (binary image) in cloud storage from the malicious insiders. Therefore, the proposed method has the benefits of simple XOR operation such as full contrast and no pixel expansion.

TABLE 1
THE (2, 2) PROBABILISTIC VISUAL CRYPTOGRAPHY (PROBVSS) SCHEME AND THE XOR-BASED WANG ET AL.'S (2, 2) SECRET SHARING SCHEME [18, 19, 32]

Secret Pixel	**Encryption Rules**		**Decryption**	
	Shadow Image 1	**Shadow Image 2**	**Stacking (OR) [18, 19]**	**XOR [32]**
□ **White**	□	□	□	□
	■	■	■	□
■ **Black**	□	■	■	■
	■	□	■	■

II. PROBLEM STATEMENT

In cloud storage, the data users (owners) are bothering about the confidentiality of their data because a data user has no control over his/her data but the cloud provider has full control on the user's data. The confidentiality is used to protect the data from insiders and outsiders attacks and therefore it ensures that only authorized users can be accessed to the data. To ensure the confidentiality of user's data in the cloud storage, a security mechanism has to be provided to the data and it should be simple and user-friendly and at the same time should be less complex. In this paper, we are introducing a new method for ensuring the data confidentiality in cloud storage based on XOR operation and XOR-based Wang et al.'s (n, n) secret sharing scheme.

III. PROPOSED METHOD

In this method, the secret image is concealed in n separate meaningful shadow images and each single meaningful shadow image is stored in different independent cloud server. For decoding the secret image, all n meaningful shadow images must be combined but less than n of them will not reveal any information about the secret image. The proposed method computes n shadow images which are made meaningful by using the public cover images and manipulates them by using simple XOR Boolean operation. Table 2 gives the truth table of XOR Boolean operation for binary inputs.

TABLE 2
THE TRUTH TABLE OF XOR BOOLEAN OPERATION FOR BINARY INPUTS

XOR ($\oplus$)	**b=0**	**b=1**
a=0	0	1
a=1	1	0

The XOR ($\oplus$) of two $N_{Row}\times N_{Column}$ binary matrices could be described by the following formulae:

$$\forall\, a_{ij} \in A,\ b_{ij} \in B, \text{where A and B are } N_{rows} \times N_{columns}$$

$$C = A \oplus B = \left[a_{ij} \oplus b_{ij}\right], i = 1,\ldots, N_{Row};\ j = 1,\ldots, N_{Column}.$$

The expression $C = A \oplus B$ means that the *ij*-th element c_{ij} of matrix *C* is equal to $a_{ij} \oplus b_{ij}$, where a_{ij} and b_{ij} are the *ij*-th elements of matrices A and B, respectively.

Our proposed method consists of the encryption (encoding) stage, the decryption (decoding) stage, the working example, the security analysis, the computational complexity, and the performance comparison with 3DES and AES methods.

A. Encryption (Encoding) Stage

The user (owner) of the secret image (SI) in this stage will compute n meaningful shadow images (B_1,..., B_n) and then store them in n different independent cloud servers. The inputs are an even integer n with n≥2, a secret data in the form of a binary (black-and-white) secret image (SI) of size N×N and a grayscale public cover image (PI) of the same size as that of the secret image (SI). The outputs of this stage are n meaningful shadow images (B_1,..., B_n) which will be stored in n different independent cloud servers. The encryption (encoding) stage is given in Algorithm 1. The process flow of components in this stage is shown in Fig. 1.

<u>Algorithm 1: Encryption (Encoding)</u>

Input: An even integer n with n≥2, a binary (black-and-white) secret image (SI) with size N×N pixels, and a grayscale public cover image (PI) with size N×N pixels and one byte per pixel (i.e., the range of pixel values from 0 to 255).

Output: n meaningful shadow images (B_1,..., B_n).

Step 1: Generate n-1 random shadow images (A_1,..., A_{n-1}), each of 0's and 1's (black and white) and size N×N pixels.

Step 2: Use XOR-based Wang et al.'s (n, n) secret sharing scheme, as shown in [32], to encrypt the black-and-white secret image (SI) into n secret shadow images (S_1,..., S_n) where each one is in the form of N×N pixels.

Step 3: Compute the first meaningful shadow image (B_1) as follows:

$$B_1 = S_1 \oplus A_1 \oplus PI$$

Step 4: Compute the intermediate meaningful shadow images (B_2,..., B_{n-1}) as follows:

$$B_i = S_i \oplus A_{i-1} \oplus A_i \oplus PI \qquad (i = 2,3,\ldots, n-1)$$

Step 5: Compute the last meaningful shadow image (B_n) as follows:

$$B_n = S_n \oplus A_{n-1} \oplus PI$$

Step 6: Store each single meaningful shadow image from n meaningful shadow images in a different single cloud server.

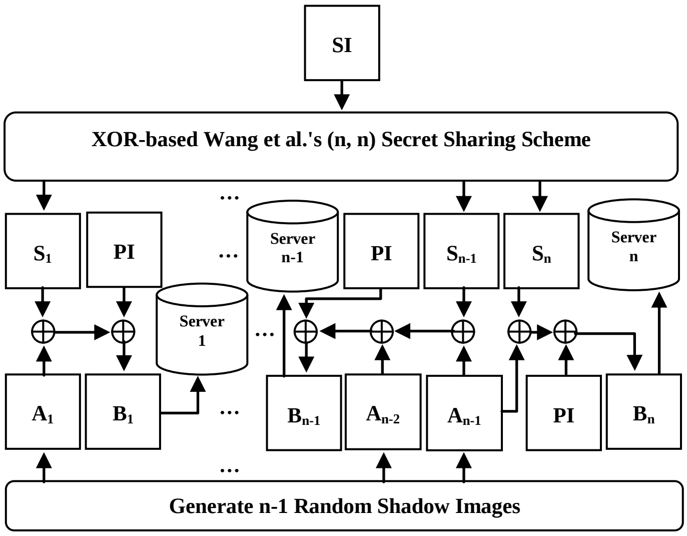

SI
XOR-based Wang et al.'s (n, n) Secret Sharing Scheme
S1
PI
Server n-1
PI
Sn-1
Sn
Server n
Server 1
A1
B1
Bn-1
An-2
An-1
PI
Bn
Generate n-1 Random Shadow Images

Fig. 1 The process flow diagram of the encryption (encoding) stage

B. Decryption (Decoding) Stage

The authorized user in this stage will get all the n stored meaningful shadow images from the n different independent cloud servers and recovery secret image by XORing the n individual meaningful shadow images. The inputs are n meaningful shadow images (B_1,..., B_n). The output is the recovered binary (black-and-white) secret image (RI) which is equal to the original secret image (SI). The decryption (decoding) stage is given in Algorithm 2. The process flow of components in this stage is shown in Fig. 2.

Algorithm 2: Decryption (Decoding)

Input: n meaningful shadow images (B_1,..., B_n).

Output: Recovered black-and-white secret image (RI) which is equal to the original secret image (SI).

Step 1: Obtain the n meaningful shadow images (B_1,..., B_n) from the n different independent cloud servers.

Step 2: Reconstruct (decode) the secret image (SI) by logical XORing the n meaningful shadow images (B_1,..., B_n) as follows:

$$RI = B_1 \oplus B_2 \oplus \cdots \oplus B_{n-1} \oplus B_n = SI$$

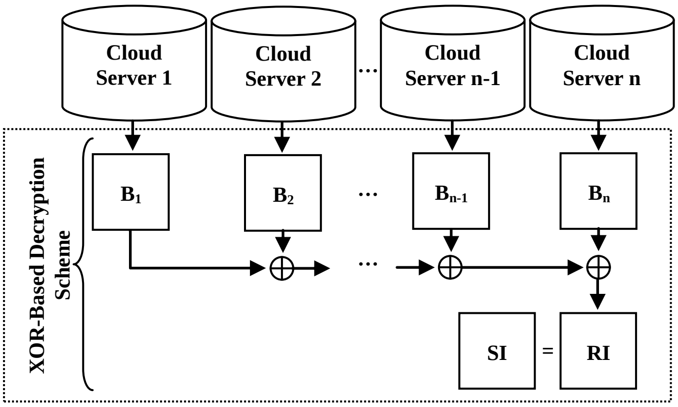
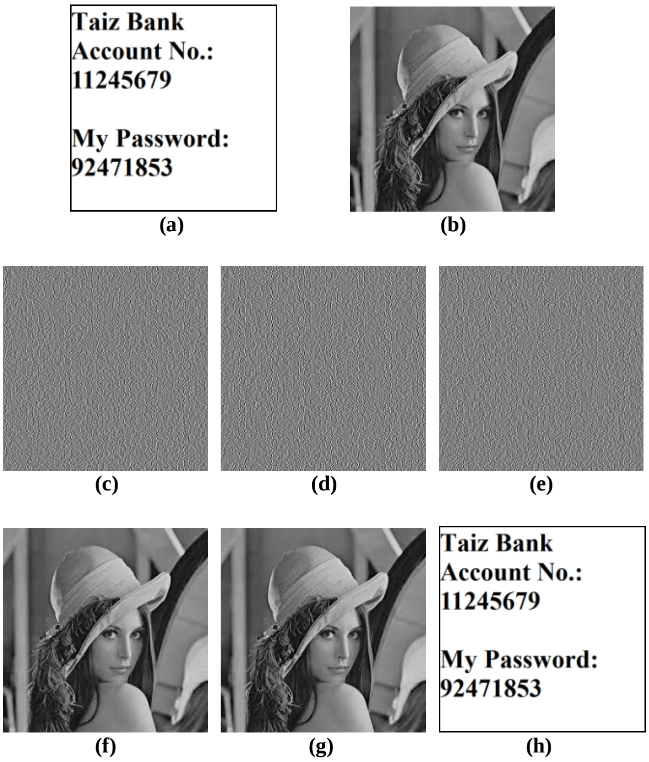


Fig. 2 The process flow diagram of the decryption (decoding) stage

C. Working Example

Fig. 3 shows a working example of the proposed method. In the encryption (encoding) stage, the user chooses an even integer n with n≥2, a black-and-white secret image (SI) with size N×N pixels and a grayscale public cover image (PI) with size N×N pixels. For simplicity it is assumed that the user chooses n=2, a black-and-white secret image (SI) with size 512×512 pixels as shown in Fig. 3(a) and a grayscale public cover image (PI) “Lena” with size 512×512 pixels and 256 gray-levels as shown in Fig. 3(b). The user generates two secret shadow images (S_1, S_2) as shown in Fig. 3(c)-(d) by applying the XOR-based Wang et al.'s (2, 2) secret sharing scheme, as shown in [32], on the secret image (SI). In addition, on the same stage, the user generates one random shadow image (A_1) as shown in Fig. 3(e). Fig. 3(f)-(g) are meaningful shadow images (B_1, B_2) after encoding. The first meaningful shadow image (B_1) is stored in first cloud server and the second meaningful shadow image (B_2) is stored in second cloud server. In the decryption (decoding) stage, Fig. 3(f)-(g) are inputs which are combined by XORing to obtain the recovered secret image (RI) given in Fig. 3(h). It can be seen that the original secret image (SI) as shown in Fig. 3(a) and the recovered secret image (RI) as shown in Fig. 3(h) are the same without any loss in contrast. Note that, the secret image (SI), the grayscale public cover image (PI), the secret shadow images (S_1, S_2), the random shadow image (A_1), the meaningful shadow images (B_1, B_2) and the recovered secret image (RI) in Fig. 3 had been resized to fit into a page.



(a) (b)

(c) (d) (e)

(f) (g) (h)

Fig. 3 Working example: (a) binary secret image SI, (b) grayscale public cover image PI, (c)-(d) secret shadow images S_1, S_2, (e) random shadow image A_1, (f)-(g) meaningful shadow images B_1, B_2, and (h) recovered secret image RI.

D. Security Analysis

Our proposed method provides security to the stored secret data at the servers in cloud computing environment. The secret image (SI) can be recovered by performing XOR operations on all n meaningful shadow images (B_1,..., B_n), but performing XOR operations on less than n of them will not reveal any information about the secret image. In order to recover the original secret image, an attacker could attempt to get the meaningful shadow images which conceal the secret shadow images of the original secret image from all different cloud servers. The security of the proposed method is therefore relies on the user's meaningful shadow images could be obtained from all different cloud servers. In addition, since each shadow image stored in cloud server is meaningful, the inside malicious attackers do not attract any attention to it. Even if inside malicious attacker gets to know one single meaningful shadow image, the others n-1 meaningful shadow images are put and stored in others n-1 far-away secured different cloud servers. Therefore, the attacker would encounter difficulties when trying to determine the user's meaningful shadow images, as long as the value of n and the size of the shadow image are chosen to be large enough. The proposed method is a paradigmatic example of using the logical random Boolean operation (XOR), which is computationally impossible, especially when using a large even integer n and large sizes of shadow images, leading to the use of a large number of the XOR Boolean operations. Therefore, the proposed method provides an ideal security system, particularly when using the proper (large) size of images (shadow images) with the right (large) value of n.

E. Computational Complexity

This subsection will be discussed two types of complexity of the proposed method, algorithm complexity and brute-force attack complexity on the algorithm. We can say that the proposed method leads to low computational complexity because it uses only the simple XOR Boolean operation which could be easily implemented by any simple and low computational device rather than complex operations. The reconstruction (encryption) stage of our algorithm computes n meaningful shadow images (B_1,..., B_n) using XOR operation, resulting in computational time proportional to n. The computational complexity of our encryption algorithm is also proportional to the image size (Z), where Z is equal to N×N pixels. Thus, the computational complexity of our encryption algorithm is $O(N^2)$ when value of n is neglected. The image reconstruction (decryption) stage of our algorithm involves XOR of all n meaningful shadow images, thus proportional to n-1. The computational complexity of our decryption algorithm is also proportional to the image size (Z). Thus, the computational complexity of our decryption algorithm is $O(N^2)$. For brute-force attack, firstly, the attacker must find all n meaningful shadow images (B_1,..., B_n) which are stored in different independent cloud servers and then getting the secret image (SI) by XORing all those n meaningful shadow images. Secondly, he/she must find all n-1 random shadow images (A_1,..., A_{n-1}) from all those n meaningful shadow images to break our proposed method and then getting any secret image in the future. The brute-force attack on the proposed method involves huge possibilities (normally in the range of 2^Z where Z is the number of pixels in the image, which is relatively a large number). Therefore, the effort and time needed for the brute-force attack to find n-1 random shadow images (A_1,..., A_{n-1}) is too consuming, especially when the number and the size of those n-1 random shadow images are large. Approximately, the time complexity of the attack is $O(2^Z)$ when value of n is neglected. Therefore, the time required for brute-force attack on the secret meaningful and random shadow images increased exponentially with the increase in the size of shadow images.

F. Performance Comparison with 3DES and AES Methods

Table 2 shows performance comparisons for the 3DES (Triple Data Encryption Standard) and the AES (Advanced Encryption Standard) encryption methods against the proposed method. The three methods were coded in C++ programming environment and run on a personal computer equipped with Intel® Core^{TM} i3 300M (2.20 GHz) processor, 2GB of RAM and Windows 2007 64bit Operating System. The user data (image) is encrypted into meaningful shadow images before they are uploaded and decrypted when they are retrieved from the cloud servers. Thus, the encryption is done in the user machine connected to the cloud servers. Time taken for encryption and decryption is calculated in the user machine. The execution time taken by the 3DES, the AES and the proposed encryption and decryption methods are calculated for different sizes of data (image). The results, as shown in Table 2, show that the proposed method has taken minimum time duration for encrypting and decrypting the data (image) of different sizes and only use n=2 when compared to the 3DES and the AES methods. From the same table, it is clear that the execution time taken for our encryption and decryption method decreases when the size of the image is decreased.

TABLE 2
PERFORMANCE COMPARISON BETWEEN THE 3DES, THE AES ENCRYPTION METHODS AND THE PROPOSED METHOD (MILLISECONDS)

Method	Size of Plaintext Block (Image)	Encryption Time (ms)	Decryption Time (ms)
3DES [33]	1024 byte (1 kb)	0.145	0.154
	65536 byte (64 kb)	9.28	9.856
	262144 byte (256 kb)	37.24	39.52
AES [34]	1024 byte (1 kb)	0.028	0.027
	65536 byte (64 kb)	1.792	1.728
	262144 byte (256 kb)	7.168	6.914
OUR	32×32 pixel (1024 byte = 1 kb)	0.0018	0.0009
	256×256 pixel (65536 byte = 64 kb)	0.1191	0.0595
	512×512 pixel (262144 byte = 256 kb)	0.4766	0.2383

IV. Conclusions

We introduced a new method to achieve and ensure data confidentiality in cloud computing storage environments using XOR operation and XOR-based Wang et al.'s (n, n) secret sharing scheme. The proposed method reconstructs the secret image exactly with full contrast, no loss of information and no randomness involved. The proposed method is simple to implement and requires comparatively lower computations because it uses only the simple XOR Boolean operations for encryption and decryption. For increasing the security, our proposed method produces n meaningful shadow images which conceal n secret shadow images of the secret image and then stores them in n different independent cloud servers instead of depending on only one (single) cloud server. The performance results show that the proposed method is highly efficient (better performance) when compared to the existing 3DES and AES encryption methods.

References

[1] P Punithavathi and S Geetha, "Visual Cryptography for Securing Images in Cloud", Chapter 15 of Book of Combating Security Breaches and Criminal Activity in the Digital Sphere, 1st ed., IGI Global, pp. 242-262, 2016.

[2] S Shubham, P S Akhilendra, "Ensuring Data Security in Cloud Storage", International Journal of Machine Learning and Computing, vol. 8, no. 4, pp. 382-386, 2018.

[3] Dr. L. Arockiam and S. Monikandan, "Efficient Cloud Storage Confidentiality to Ensure Data Security", International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03–05, pp. 1-5, 2014.

[4] Dr. L. Arockiam and S. Monikandan, "A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage", International Journal of Engineering Research & Technology (IJERT), vol. 3 issue 12, pp. 1053-1058, 2014.

[5] V Maheshwari, "Data confidentiality and keyword search in the cloud using visual cryptography", Master Thesis, School of Computer Science, McGill University, Montreal, Canada, 2011.

[6] K Brindha and N Jeyanthi, "Securing Cloud Data using Visual Cryptography", IEEE Conference on International Conference on Innovation Information in Computing Technologies (ICIICT), pp. 1-5, 2015.

[7] S. S. Hegde and R Bhaskar, "Cloud Security Using Visual Cryptography", International Journal of Distributed and Parallel Systems (IJDPS), vol.3, no.1, pp.9- 13, 2012.

[8] Dr. L. Arockiam and S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, pp 3064-3070, 2013.

[9] Er. Supriya Kinger, "Efficient Visual Cryptography", Journal of Emerging Technologies in Web Intelligence, vol. 2, no. 2, pp. 137-141, 2010.

[10] W Stallings, "Cryptography and Network Security: Principles and Practices", New Delhi: Prentice-Hall, Inc, 4th Edition, 2006.

[11] M Naor and A Shamir, "Visual Cryptography", Advance in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science, Springer-Verlag, 950, pp. 1-12, 1995.

[12] A Jaafar and A Samsudin, "A New Visual Public-Key Cryptosystem Based on Non-Expansion Technique and Boolean Operations", Ph.D. Thesis, School of Computer Sciences, USM, Peneang, Malaysia, 2011.

[13] A Jaafar and A Samsudin, "A Survey of Black-and-White Visual Cryptography Models", International Journal of Digital Content Technology and its Applications (JDCTA), vol. 6, no. 15, pp. 15-28, 2012.

[14] W Hawkes, A Yasinsac and C Cline, "An Application of Visual Cryptography to Financial Documents", Technical Report TR001001, Florida State University, 2000.

[15] I Fischer and T Herfet, "Visually Authenticated Communication", Proceedings of 8th International Symposium On Systems and Information Security, Brazil, pp. 471–474, 2006.

[16] J Pejaś and M Zawalich, "Visual Cryptography Methods as a Source of Trustworthiness for the Signature Creation and Verification Systems", Advances in Information Processing and Protection, Springer-Verlag, USA, pp. 225-239, 2008.

[17] C.-S. Hsu, "A Study of Visual Cryptography and its Applications to Copyright Protection Based on Goal Programming and Statistics", Ph.D. Dissertation, Department of Information Management, National Central University, 2004.

[18] R Ito, H Kuwakado and H Tanaka, "Image Size Invariant Visual Cryptography". IEICE Trans. Fundam. Elect. Commun. Comput. Sci., E82-A(10), pp. 2172-2177, 1999.

[19] C.-N. Yang, "New Visual Secret Sharing Schemes Using Probabilistic Method", Journal of Pattern Recognition Letter, 25, pp. 481-494, 2004.

[20] R Sinha and M Shrivastava, "XOR Operated Visual Cryptography", Mathematical Sciences International Research Journal, vol. 1, no. 1, pp. 343-348, 2012.

[21] N Soman and S Baby, "XOR-Based Visual Cryptography", International Journal on Cybernetics & Informatics (IJCI), vol. 5, no. 2, pp. 253-264, 2016.

[22] D Gayathri and Dr T Gunasekran, "Design of XOR based visual cryptography scheme", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), vol. 4, issue 2, pp. 367-370, 2015.

[23] X Jiang, Z Lu and X Ding, "A Semi-Fragile Blind Watermarking Scheme for Color Images Based On Visual Cryptography and Discrete Cosine Transform", International Journal of Innovative Computing, Information and Control, vol. 13, no. 5, pp. 1709-1719, 2017.

[24] W Dang, M He, D Wang and X Li, "K out of K Extended Visual Cryptography Scheme Based on "XOR"", International Journal of Computer and Communication Engineering, vol. 4, no. 6, pp. 439-453, 2015.

[25] B Raja Koti, K. Naveen Kumar and Dr. G.V.S. Raj Kumar, "Secret Image Sharing Technique based on Bitwise XOR", IJCSET, vol. 6, issue 5, pp. 138-143, 2016.

[26] A Ross and A Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, 2011.

[27] A Nayan Ardak and Prof. Avinash Wadhe, "Visual Cryptography Scheme for Privacy Protection", International Journal of Computer Science and Information Technologies, vol. 5 (2) , pp. 2026-2029, 2014.

[28] F Liu and C Wu, "Optimal XOR based (2,n)-Visual Cryptography Schemes", State Key Laboratory Of Information Security, Institute of Software Chinese Academy of Sciences, pp. 1-20, 2010.

[29] K Brindha and N Jeyanthi, "Secured Document Sharing Using Visual Cryptography in Cloud Data Storage", Cybernetics And Information Technologies, vol. 15, no. 4, pp. 111-123, 2015.

[30] M Mulay, R Surana and Y Tibdewal, "Enhanced Security in Multi Cloud Using Visual Cryptography and Secret Sharing", International Journal of Allied Practice, Research and Review (IJAPRR), vol. II, issue II, pp. 53-57, 2015.

[31] V Matte1 and L. Ravi Kumar, "A New Framework for Cloud Computing security using Secret Sharing Algorithm over Single to Multi-Clouds", International Journal of Computer Trends and Technology (IJCTT),vol. 4, issue 8, pp. 2820-2824, 2013.

[32] D Wang, L Zhang, N Ma and X Li, "Two secret sharing schemes based on Boolean operations", Pattern Recognition, vol. 40, no. 10, pp. 2776–2785, 2007.

[33] Code Taken From: https://www.techiedelight.com/3-des-implementation-c/

[34] Code Taken From: https://codereview.stackexchange.com/questions/179930/aes-implementation-in-c