IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

An Efficient K-N Secret Sharing Image and AES Encryption Algorithm in Visual Cryptography

Vignesh. M[1], Raihana. P.A[2], Shahadha Hakkim[3], Sukanya. S[4]

Assistant Professor, Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India[1]

Student, Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India[2,3,4]

Abstract: Nowadays, many researchers proposed algorithms based on the combination of visual cryptography method with the aim of high secure secrecy, reliability, accuracy and efficiency for the secret message. Visual cryptography provides high security with less computation when comparative with other methods. The proposed system takes any image which is to be shared secretly. This image is encrypted using a key given by the user. Further, the encrypted image is divided into N different shares using K N Secret Sharing Algorithm. These N shares can be distributed but, the end user needs only K of these shares to generate the original image. After the original image is generated it is still in encrypted form. AES Cryptographic techniques is to protect the image. The image is encrypted using AES algorithm encoding schema has been proposed to convert the key into shares based on Visual Secret Sharing. The key which is used to encrypt the image originally is now required again to decrypt it, thus providing an additional level of security.

Keywords: AES, Visual Cryptography, Image Encryption.

I. INTRODUCTION

The primary objective of image encryption is to transmit an image securely over a connected network so that no unauthorized user should be able to decrypt the image. Image encryption has applications in many fields including Banking, Telecommunication and Medical Image Processing etc. Encryption has become an important part due to the emergence of Internet, where sending and receiving data across computers need security of some standard. Various algorithms have been proposed in this field to encrypt and decrypt images.

Cryptography is about constructing and analysing protocols that prevent public from reading secret messages. Data hiding technique is the existence of the secret message. In other words, it involves hiding the information in such a way that it appears no information is hidden at all. Hence, when we combine cryptography, it results a powerful tool which enables the people to transmit sensitive data over the internet securely, by preventing eavesdrop attack even knowing that there is a form of communication. Neural networks are used to identify the best locations with high energy coefficients so that embedding is done over those locations. By doing so, the quality of the image would be as good as the original image. Visual cryptography is a unique technique where data is hidden in images and these images are split into number of shares during encryption. During decryption, these shares are overlapped into one another to get back the original image. No special decoding schemes are needed, just human visual system is sufficient. Thus, by image visual cryptography, it adds lot of challenges to identify encrypted data for the intruders, thus providing additional layer of security for the secret data.

In a sharing phase, each party receives a transparency containing a printed image, which looks like a collection of black and white random pixels. The transparency does not leak any information about the secret image. In a reconstruction phase, when a properly chosen subset of transparencies are superposed and perfectly aligned, the secret image is reconstructed. The peculiarity of the technique is that the human visual system performs the reconstruction process: no machinery, computing mathematical operations, is required. Hence, it can be used by everyone: once the transparencies have been generated and privately distributed, cryptographic tools or skills are not needed to reconstruct the secret image.

Visual cryptography method is only applied to black, white pixels until 1997. The existing system which contributes the complex parallelism mechanism to protect the information by using (DES) Technique. DES is an encryption algorithm which uses 64 bit as a data and generates a secured data. In Encryption, when cipher key is inserted, the plain text is converted into cipher text by using complex parallelism. Similarly, in decryption, the cipher text is converted into original one by removing a cipher key. The complex parallelism technique involves the process of Substitution Byte, Shift Row, Mix Column and Add Round Key. The above four techniques are used to involve the process of shuffling the message. The complex parallelism is highly secured and the information is not broken by any other intruder.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

II. RELATED WORK

Visual Cryptography is for Data Hiding in image through Wireless Network. Methodologies followed are i) Data Encryption using any Encryption algorithm ii) LSB is used for hiding the secret data in the cover image iii) genetic algorithm is used to reshuffle the modified image bits, so as to ensure better security iv) visual cryptography is applied at the end to secure transmission of the image over the internet. Advantages are i) this project resulted in better results in terms of image quality and steganalysis, ii) security features are highly optimized as genetic algorithm is used for reshuffling the bits iii) visual cryptography ensures the secured transmission of the image over the internet. Future scope would be i) could be towards adding public/ private key for encryption ii) face recognition facility for user to introduce more security.

S. Premkumar and R. Swathiramya prove that optimal Contrast Grayscale visual cryptography with modified multi-secret sharing for secure application. Methodology involves i) hiding the secret information in the edges rather than the smooth areas of a cover image ii) Multiple Base Notational Systems (MBNS) is used. Advantages are i) MBNS serves more security, best values in terms of performance, quality metrics in comparison BPCS, PVD. Future scope would be towards adding face recognition facility for user to introduce more security.

Moushmee Kuri and Dr. Tanuja Sarode Random key share overlapping(RKO) technique for Visual Cryptography. Methodology involves i) LSB method is applied for image hiding ii) RKO technique is used to split stego image into random share and key share at the sender side. At the receiver side i) random share and key share are overlapped using XOR method to form single image or stego image ii) reverse image cryptography is applied to get back the original image. Advantages are i) perfect reconstruction property, the revealed data and the cover image are exact replica of the original ii) can be used by forensic and security investigators to hide/detect suspicious data iii) less storage & less amount of computation time iv) VC ensures it's impossible for the attacker to even guess that the transmitted shares would contain some hidden data. Future scope would be towards adding user authentication using password and/or photo.

Monu U. Ragashe1 and Sneha M. Ramteke2 did good research on image visual cryptography algorithms and their findings are listed under the title "the visual cryptography in computer forensics". Various steganographic techniques explained are LSB, Dynamic Compensation LSB, Video, audio, image, text types. Various visual cryptographic techniques explained are threshold Image Hiding Scheme, Image Size Invariant VC, joint visual cryptography and waterfall (JVW) method, region incrementing visual cryptography(RIVC). Advantages are i) The importance of VC with respect to security are highlighted ii) better performance of visual cryptography with respect to cryptography is explained. Future scope is to invent some more efficient and effective image and VC techniques. S. R. Navale, S. S. Khandagale, R.

A. Malpekar, Prof. N. K. Chouhan came up with an approach for Secure Online transaction using Visual Cryptography. Methodology involves information submitted by the consumer to the online website at merchant's site is minimized by providing only minimum information that will only verify the payment made by the consumer from his account. This is accomplished by the introduction of a central Certified Authority (CA), visual cryptographic (k, n) threshold RG-based VC technique. Advantages are i) minimizes consumer information sent for TRANSACTION OF FUNDS to the online merchant's website ii) prevents illegal use of consumer information at merchant's website iii) Presence of a fourth party, CA, enhances consumer's fulfilment and security. Future scope would be i) he payment system can also be extended to internet or physical banking ii) shares may contain consumer image or signature in addition to consumer authentication password.

S. R. Khonde, Dheeraj Agarwal and Shrinivas Deshmukh propose "Online Payment System using BPCS Visual Cryptography". Methodology involves providing least information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of BPCS Visual Cryptography. LinkGuard Algorithm is also used. Advantages are i) provides customer data privacy, prevents misuse of data at merchant's side ii) BPCS is highly effective against eavesdropping and has a high information hiding capacity as compared to traditional cryptography approach iii) prevention of identity theft and customer data security iv) consumer satisfaction and authorized merchant-bank interaction. Future scope is to apply the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

Srinivasan nagaraj et al. The enlarged size of the internet and vast communication across it and also medical needs digital images require of security plays vital role. New encryption technique Using elliptic curve cryptography with magic matrix operations for securing images that transmits over a public unsecured channel. There are two most important groups of image encryption algorithms: some are non-chaos-based selective methods and chaos based selective methods.

Xuehu Yan et al have proposed three general threshold construction methods from specific cases. The constructed threshold VCSs are also progressive VCS without the pixel expansion. The shadow images (Shares) are random noise-like, hence the authors proposed CVCS has no cross interference of secret image in the shadow images. From the progressive visual quality of the authors, covered secret image can be gained for the CVCS. When the shadow images

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

are collected, cannot retrieve any information of the secret image could be recognized, which shows the security of the CVCS.
Paulius Palevicius et al presented the integration of dynamic visual cryptography technique based on the inter play of visual cryptography and time averaging geometric with Gerchberg–Saxton algorithm. The authors made study on the stochastic grating, which is used to embed the secret into a single cover image. The hidden information can be visually decoded by a naked eye if only the amplitude of harmonic oscillations corresponds to an accurately preselected value. The visual image encryption scheme is based on computer generated holography, optical time averaging and principles of dynamic visual cryptography were provided by the authors.

III. PROPOSED APPROACH

The AES algorithm has a block size of 128 bits. It supports three different key lengths of 128, 192 and 256 bits. AES replaced Data Encryption Standard and it is now used worldwide. In AES there is no Feistel Network as opposed to the previous standard DES. The cipher consists of rounds, where the number of rounds depends on the key length: 10 rounds for a 128-bit key, 12 rounds for 192 bits key, and 14 rounds for a 256-bit key. The whole algorithm operates on a 4 x 4 matrix of bytes. The first rounds consist of four distinct transformation functions: Sub Bytes, Shift Rows, Mix Columns, and Add Round Key. The final round contains three transformations. The Mix Columns function is not used in the final round. Each transformation takes one or more 4x4 matrices as input and produces a 4x4 matrix as output. Provided that all the four rounds are reversible, it is easy to prove that decryption does recover the plaintext.

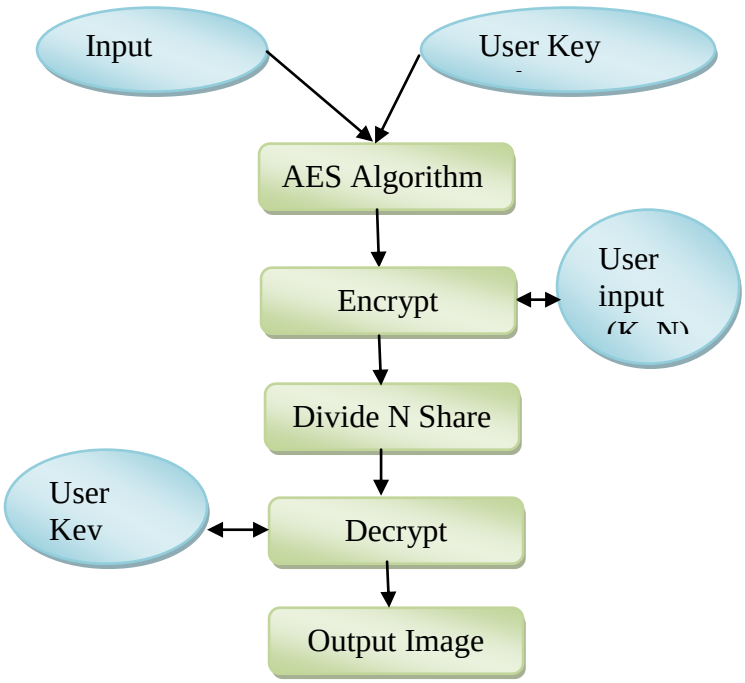

Fig. 1Propose architecture diagram

As seen from the above information, both AES are vulnerable to certain attacks and therefore are not suitable for Image Encryption. In order to achieve such security standard, the best parts of both the algorithms are combined to work together. The proposed algorithm is divided into two phases.

A. Encryption Phase
B. Decryption Phase.

A. Shares Creation Scheme
The RGB pixel values are taken from the original image and the separate matrix (Original matrix) and (R_i, G_i, B_i). Generate globalized key matrixR_M where M=1,2, 3…255. The division takes place into n number of shares and then distribution of shares is done among n persons. The secret can be recovered if and only if k or more of these persons i.e. k<=n bring their shares together. However, if the number of persons is k-1 then secret reconstruction will fail.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

B. Shares Encryption

AES algorithm consists of the following four base procedures. Sub Bytes Transformation: The SubBytes () transformation is a non-linear byte substitution that operates independently on each byte of the state using a substitution table. Shift Rows Transformation: In the Shift Rows () transformation, the bytes in the last three rows of the state are cyclically shifted over different number of bytes. The first row will not get shifted. Mix Column Transformation: In Mix Column (), the columns of the state are considered as polynomial and then multiplied by modulo with fixed polynomial, individually. AddRoundKey Transformation: In the AddRoundKey () transformation, a round key is added to a state by a simple bitwise XOR operation. Each round key consists of Nb words from the key schedule; those Nb words are each added into the columns of the state. To encrypt the shares the input is considered as a share. Hence, the shares are taken that is converted into block matrices. During the encryption process, the shares are undergone to the basic procedure of AES algorithm and the output is encrypted share. In this process, shares and AES algorithm binds together to give the resultant shares are called the encapsulated shares.

Input: Encrypt - (I), (K), (N)
Output: (CI), 1, 2… N (KI)
Here I – Image to be encrypted. Supports various standard formats.
K – Key File given as a sequence of characters.
N – Number of shares of Key to be generated (min 2)
CI – The base64 encoding of the encrypted image I.
KI – N images or shares of the Key that are generated.

Algorithm (with N = 8):
Step 1. Read the input image and encode it using base64 standard.
Step 2. Read the key file and initiate the AES 256-bit key file.
Step 3. Encrypt the image using the base 64 encoded text and hash generated in steps 1 and 2 respectively.
Step 4. Create a new Image C of size (w, h) with pixel data p where
a. w - character support for key file (Default: 255)
b. h – Number of characters in the key file
c. p – Pixel Data to be filled (Default: 0)
Step 5. For-each row i in height of image repeat:
a. Let j be ASCII code of the ith character in the key file.
b. Fill the first j pixels of the image in the ith row with black color.
i. C [i] [j] = 0 for every i, j in h, w such that j <ASCII(key[i])
Step 6. Create N (= 8) Images (R, P) of the same size (w,h) and pixel data such that
a. For the first image R, pixel data is generated randomly. It can be either 0 (black) or 1 (white). i. R [i] [j] = random(0, 1)
b. Second image pixel data P [i] [j] is defined such that i. P [i] [j] = R [i] [j] xor C [i] [j] for every i, j in (h, w)
Step 7. Output the encrypted encoding CI, Images P and R respectively.

C. Shares Decryption

The rounds of the decryption algorithm are governed by the following four stages namely the Inverse Shift rows, Inverse Substitute Bytes, Add round key and Inverse Mix columns steps. The inverse AddRoundKey step was eliminated. AES decryption occurs simply as the reverse order of encryption. The encrypted shares are now fed as the input blocks, in which the inverse shifting of the rows value is taken place. It is then followed by the inverse substitution of the pixel positions along with the Key value. Finally, the inverse mix column step was taken place. The resultant image thus produced was the original image at the time of share creation. During the decryption process, the encapsulated shares are extracted by decryption process of AES Algorithm to retrieve the share 1 and share8.

Input: (CI), 1, 2… N (KI)
Output: I Here
CI – Base 64 encoded cipher text.
KI – N shares of the Key that must be supplied for decryption. I – Decrypted Image

Algorithm (with N = 8):
Step 1. Read the input cipher text of the image CI.
Step 2. Load the Images K1, K2 from the input KI.
Step 3. Create a new Image CK of size (w, h) same as K1, K2 such that
a. CK [i] [j] = K1 [i] [j] xor K2 [i] [j] for every i, j in (h, w)
Step 4. Initialize key K as an array of characters of size same as height of image CK (h).

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

Step 5. For-each row i in height of image CK repeat:
a. Let count = 0
b. For each pixel j of the image in the ith row with black color.
i. increment count by 1
c. Find the character ki by using ASCII code of the count generated after b. i.e., ki =char(count)
d. Set K[i] = ki
6. With the Key K initialize the AES 256 Algorithm with hash(K)
Step 7. Decrypt the cipher text CI and save the decrypted base64 encoding as an Image I
Step 8. Output the decrypted image I.

D. Shares Reconstruction Scheme

Figures Finally, all decrypted shares are stacked (Combine these (R1, R2) (G1, G2) and (B1, B2) matrices) together to retrieve the secret image. Only if all the numbers of secret shared images are stacked together, it is possible to reveal the secrets. If any one of the shares of the original image is missing, it is impossible to retrieve the original image. The decryption process consists of two steps. First step is done by human visual system where at least k number of shares out of n number of shares is superimposed to give reconstructed image.

- Input the number shares you have and the same key used for encryption.
- Shares should be equal to k or greater than k
- Perform the bitor operation on converted shares to get reconstructed encrypted image.
- Now XOR the reconstructed encrypted image and converted key to get 24-bit decrypted image, it then reconstructed to give decrypted image equal to original image.

Human visual system acts as an OR function. For computer generated process, OR function can be used for the case of stacking k number of shares out of n. Second step is decryption of reconstructed image, where pixel array is computed from reconstructed image and XOR with same key used for encryption. Decrypted image is exactly equal to original image.

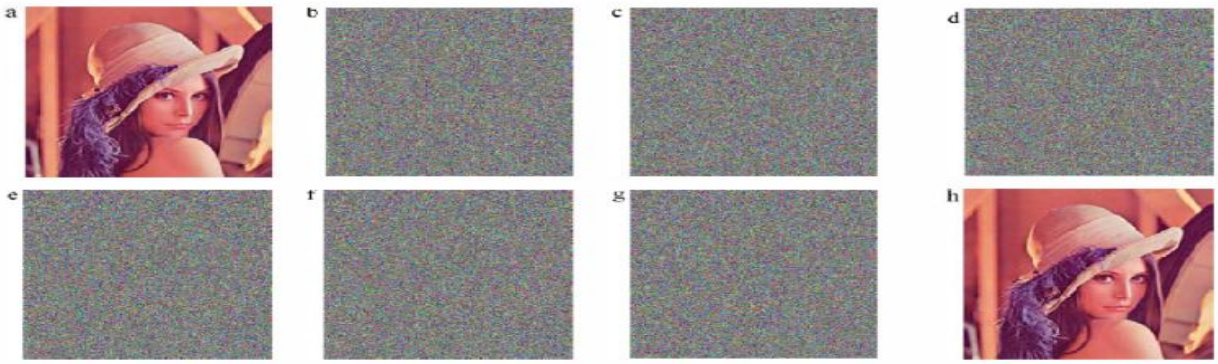

Fig. 2. (a) Secret image; (b, c) Shares (d, e) Encrypted Shares; (f, g) Decrypted Shares; (h) Stacked Images.

IV. EXPERIMENTAL RESULTS

In order to test the proposed methods a test bed of 100 images was created. The databases used are the UCID dataset and test images widely used in experiments etc. Initially we have taken a 256×256 grayscale image as original image. The sizes of the shares are same as that of the original image. Above table shows the results of Embedding and extracting secret data in the shares using proposed visual cryptography and advanced encryption standard.

A. Shares Reconstruction Scheme

Image encryption is a conversion of secret image into scrambled image. The image quality may be differing from secret image to encrypted image depending on the encryption algorithm. High PSNR (Peak Signal to Noise Ratio) indicate a lower variation between the original (without noise) and reconstructed image. The major benefit of this measure is simplicity of computation, but it does not reflect perceptual quality of the image.

TABLE IPSNR (IN DB) VALUES FOR EXISTING SYSTEM

Image Name	**Existing Shares Generation**	
	Share 1	Share N
Lena	8.78	8.78
Baboon	8.81	8.81

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

TABLE IIPSNR (IN DB) VALUES FOR EXISTING SYSTEM

Image Name	Existing Shares Generation	
	Share 1	Share N
Lena	8.84	8.80
Baboon	8.82	8.84

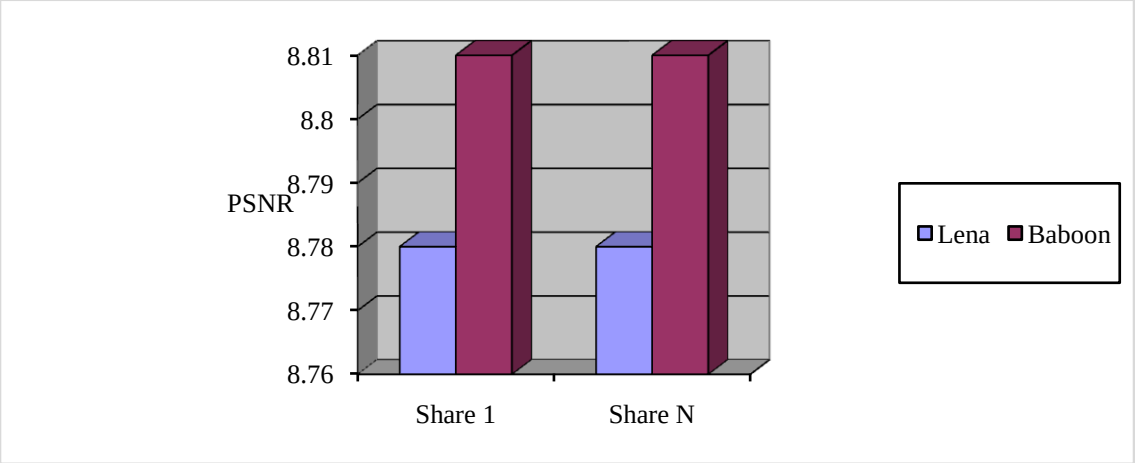

Fig. 3 PSNR compare of existing system with N Share

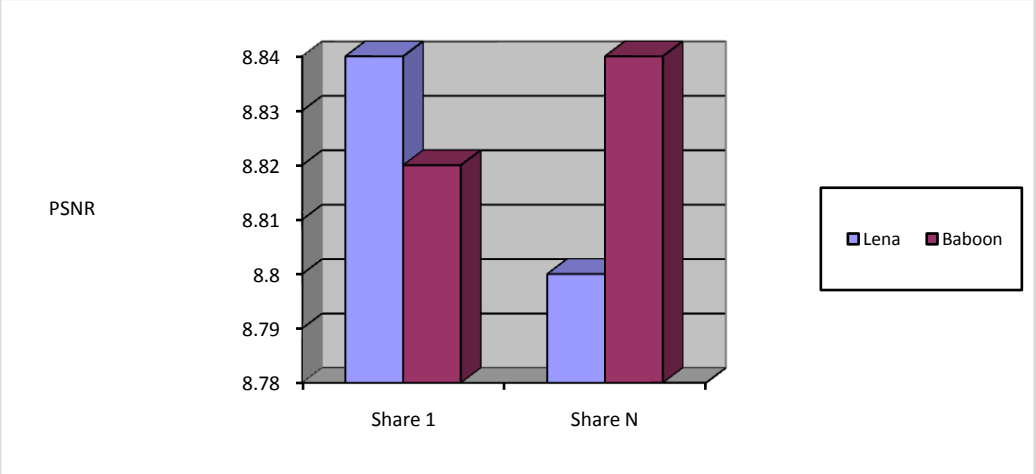

Fig. 4PSNR compare of proposed system with N Share

The proposed scheme with their PSNR is employed for various sample test images. As per PSNR understanding with original image and decrypted image, the value should be higher. It shows the better for its superiority. When the PSNR value is compared for the original image with encrypted image, the PSNR is low which yields better encryption quality

V. CONCLUSION

The cryptographic methodology proposed in this paper has been tested on different types of input images with change in size of the image and keys of AES encryption algorithm. The entire time secret image is retrieved with good visual quality. In fact, there is no observable change in the quality of image, since the image processing is mostly done on the key images and its shares. The propose algorithm k-n secret sharing scheme an image is divided into n number of shares in such a way that the original image is retrieved by stacking at least k number of shares, where k and n. As future work, this scheme can possibly be modified to use color image in place of binary image for the key and then generate the shares using Visual Cryptography. Improvement in the quality of key share images can be done i.e., a meaningful image instead of normal binary image. More sophisticated public key encryption can be used to reduce key size and cipher text size. Image processing attacks like translation, rotation and scaling of key shares can also be controlled.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

REFERENCES

[1] Pakshwar, Rinki, Vijay Kumar Trivedi and Vineet Richhariya. "A survey on different image encryption and decryption techniques.", IJCSIT) International Journal of Computer Science and Information Technologies 4.1, 2013.
[2] Kumar, M. Arun, and K. Jhon Singh, "Novel Secure Technique using Visual Cryptography and Advance AES for images.", International Journal of Knowledge Management and e-learning, Vol. 3, No. 1, pp. 29-34, 2011.
[3] Nikita, Ranjit Kaur, "A Survey on Secret Key Encryption Techniques", Impact: International Journal of Research in Engineering & Technology IMPACT: IJRET, May, 2014.
[4] Chang, C. C. and Yu. T. X., "Sharing a Secret Gray Image in Multiple Images, in the Proceedings of International Symposium on Cyber Worlds: Theories and Practice", Tokyo, Japan, Nov. 2002.
[5] M. Naor and A. Shamir, Visual cryptography. "Advances in Cryptology" EUROCRYPT '94, 1995
[6] C. Chang, C. Tsai, and T. Chen, "A new scheme for sharing secret color images in computer network"., International Conference on Parallel and Distributed Systems, July 2000.
[7] E. Verheul and H. V. Tilborg., "Constructions and properties of k out of n visual secret sharing schemes. Designs", Codes and Cryptography, 1997.
[8] C. Yang and C. Laih., "New colored visual secret sharing schemes. Designs", Codes and Cryptography, 2000.
[9] Kulvinder Kaur and Vineeta Khemchandani, "Securing Visual Cryptographic Shares using Public Key Encryption", Advance Computing Conference (IACC), Feb, 2013
[10] Orr Dunkelman, Nathan Keller⋆, and Adi Shamir, "Improved Single-Key Attacks on 8-round AES-192 and AES-256", ASIACRYPT, LNCS, 2010.
[11] Alex Biryukov, Dmitry Khovratovich, Ivica Nikolić, "Distinguisher and Related-Key Attack on the Full AES-256", Advances in Cryptology - CRYPTO 2009
[12] Joan DAEMEN, Vincent RIJMEN, "On The Related-Key Attacks Against AES", Proceedings of The Romanian Academy, Series A, 2012
[13] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir, "Key Recovery Attacks of Practical Complexity on AES Variants with up to 10 Rounds", Cryptology ePrint Archive, 2009
[14] Andrey Bogdanov⋆, Dmitry Khovratovich, and Christian Rechberger⋆, Biclique Cryptanalysis of the AES-192 and AES-256, "International Conference on the Theory and Application of Cryptology and Information Security", 2009.
[15] S. Parker., L. O. Chua., "Chaos: a tutorial for engineers. Proceedings of the IEEE", vol. 75, no. 8, pp. 982–1008, 1995
[16] W.Wu .,N. F. Rulkov., "Studying chaos via 1-Dmaps—a tutorial. IEEE Trans. on Circuits and Systems I Fundamental Theory and Applications", vol. 40, no. 10, pp. 707–721, 1993
[17] Chin-Chen Changa, Min-Shian Hwangb, Tung-Shou Chenc, "A new encryption algorithm for image cryptosystems", 2000
[18] Y.-Q. Zhang, X.-Y. Wang "Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation", 2014.
[19] Y.-Q. Zhang, X.-Y. Wang "A new image encryption algorithm based on non-adjacent coupled map lattices", 2015.
[20] H. Liu, X. Wang "Color image encryption based on one-time keys and robust chaotic maps" 2010