International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

K-N Secret Sharing Scheme Encrypting Multiple Images in Visual Cryptography

Anu G S[1], Geethos Ninan[2]

[1]M. Tech Scholar, Department of Electronics and Communication Engineering, MBCCET, Idukki 695015, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, MBCCET, Idukki 695015, India

Abstract: ***Cryptography is necessary for secure information as the relevance of security is increasing day by day with advent of e-commerce. The security of digital images is principal vicinity of situation, especially while we address digital images in which it can be saved or send via the communication channel. The AES is generally used encryption algorithm in diverse security application. The key generation will happen by significant components of genetic algorithm. Genetic algorithm is class of optimization algorithm which can be utilized to solve various issues through displaying a rearranged adaptation of genetic process. The proposed framework takes any image which is to be secretly shared. This image is encrypted using a key given by the user and data embedded using genetic algorithm. These N shares can be appropriated as it may the end user needs just K of these shares to produce the original image. Along these line gives an extra degree of security.***

Keywords: Visual cryptography, AES, Genetic algorithm, K-N secret sharing scheme

1. Introduction

The main objective of image encryption is to transmit an image safely over an associated system so that no unapproved user ought to have the option to decrypt the image. Image encryption has application in numerous fields. Encryption has become a significant part due to rise of internet, where sending and accepting information across pcs needs security of some standards. Different algorithm has been proposed right now to encrypt and decrypt image.
Visual cryptography is a one kind strategy where information is covered up in pictures and these pictures are part into number of shares during encryption, these shares are covered into each other to get back the original image. No uncommon unraveling plans are required, simply human visual framework is adequate along these lines, by image visual cryptography, it adds part of difficulties to distinguish encrypted information for the interlopers, in this manner giving extra layer of security for the mystery information. Here same key is utilized for encryption and decryption. Symmetric key cryptography is one of the most significant sorts of cryptography were key is shared between both imparting parties. Symmetric key cryptography is utilized for private encryption of information to accomplish elite.

The AES is broadly utilized encryption algorithm in diverse security applications. The AES standard uses key size of 128, 192 and 256 pieces to give progressively verify information. AES creates keys through the properties of the Rijndael algorithm rather than traditional strategy for the key generation.

Genetic algorithm is a class of advancement algorithm which finds the appropriate fittest answer for a given issue from a population. It depends on natural selection, inheritance, mutation and crossover. Mutation and crossover are the operators of the genetic algorithm. A (K,N) secret sharing scheme is a common case of the secret sharing schemes, this is a technique for sharing a secret among N members so that any K or more members can recover the secret with their shares, However no K-1 or less members can acquire any information about the secret from their shares.

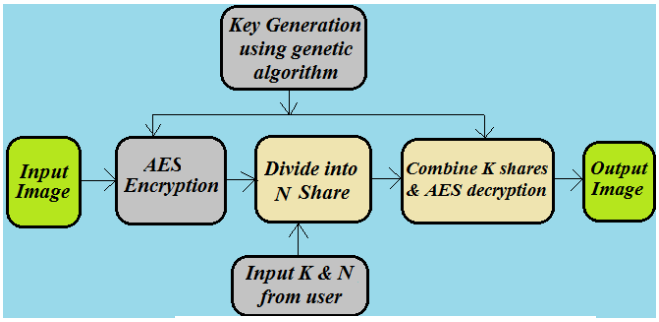

Figure 1: Block diagram of proposed frame work

2. Related Works

The following are the papers surveyed. MATLAB is used here to evaluate the performance of the system. Genetic algorithm is used to produce a new encryption method by exploiting the powerful features of the crossover and mutation operations of (GA). It is a new approach of genetic algorithm with pseudo random sequence to encrypt image stream. The feature of this approach includes high security and high feasibility for easy integration with digital image transmission applications.it achieves a high throughput rate required for real time data protection [3].

A crypto analysis technique and genetic algorithm-based strategies are mainly used in the field of cryptography. The attention was an old-style cipher, including substitution, change transposition, ruck stack and vernam ciphers. The standards utilized in these cipher structure establish for huge number of the cutting-edge cryptosystem. A significant number of the GA based attaches needed data required for correlation with the conventional attaches elapsed time on parameters one of a kind to one GA based attach doesn't take into account successful examination among the contemplated approaches. The rational and apparently

substantial GA based attack were executed with the goal that a predictable, sensible arrangement of measurements [4].

There is a sort of similarity in pixels are changed positions or the blocks are confused or the self-assertive bits are added to the pixels so as to encrypt the image. The image encryption is finished utilizing breaking and converging of bits. The image is first separated into squares otherwise called grid. Image are used to find the pixels and further genetic algorithm is utilized to encode the image utilizing one-point traverse. Framework is randomized by utilizing a huge capacity pool and utilizing capacities from those. More than one capacity is utilized to scramble the pictures. Hence some sort of randomness is introduced in the mechanism there increasing its key length. The vernam cipher includes XOR operation of the first bit with second bit and so on. it starts with the least significant bit and proceeds throughout the entire word length. Since vernam cipher is the only efficient cipher or unbroken cipher. The algorithm is comparatively more effective and less complex compared to existing spatial domain technique [5].

Classification of electronic information is transmitted over the web. Information encryption is generally used to guarantee security of information. Genetic algorithm, are a class of streamlining calculations. Numerous issues can be illuminated utilizing genetic algorithm through displaying an improved rendition of genetic procedures. Genetic algorithm with pseudorandom capacity to scramble and decode information stream. proposed hereditary calculation based secret key encryption strategy. The encryption procedure is applied over a double record with the goal that the calculations can be applied over a text just as mixed media information. Pseudorandom number generator used to create pseudorandom sequence of numbers for encryption and decoding strategy. Utilizing three sort of hybrid activity. Balancing the pseudorandom sequence by three the hybrid activities will execute by grouping for mutation activity, utilizing flip bit mutation technique.in the calculation, have essentially utilized five keys: one is for separating the plane content in to squares. Second is for creating pseudo random arrangement for hybrid activity. Third is for producing another pseudo random grouping, fourth key is for regulate the succession and last one is for change activity. this encryption procedure is performed on two-fold information. Subsequently, this strategy can be applied to scramble any configurations of information like content, pictures, sound and numerous information. the two-fold information is partitioned in to obstructs, the encryption and unscrambling strategy can be done [6].

An extended visual cryptography scheme (EVCS), for an access structure on a lot of n members, is a method to encode n pictures so that when we stack together the transparencies related to members in any set X∈ΓQual we get the secret message with no hint of the first pictures, however any X∈ΓForb has no data on the common picture. After the first pictures are encoded, they are as yet important, that is, any client will perceive the picture on his straightforwardness. This yields a fundamental and adequate condition for the presence of (k; k)- edge EVCS for the estimations of such differences. A general strategy to actualize EVCS, which utilizes hyper graph colorings. This strategy yields (k; k)-limit EVCS which are ideal as for the pixel development. Uses of this procedure to different intriguing classes of access structures by utilizing pertinent outcomes from the hypothesis of hyper diagram shading [7].
In a (k, n) visual cryptography scheme (VCS), a mystery picture is encoded into n shadow pictures that are appropriated to n members. Any k members can uncover the secret picture by stacking their shadow pictures, and not as much as k members have no data about the secret picture. At the point when the secret picture is multiple and this is a purported multi-secret VCS (MVCS). The past takes a shot at MVCS are for the most part the basic 2-out-of-2 cases. a general (k, n)- MVCS for any k and n. Three fundamental commitments: first broad (k, n)- MVCS, which can be applied on any k and n, the conventional security and differentiation states of (k, n)- MVCS and hypothetically demonstrate that the (k, n)- MVCS fulfills the security and difference conditions. By extending a secret pixel into m sub pixels. In the reproduced picture, the diverse whiteness is utilized to recognize the dark shading from the white shading. As a matter of fact, the measures of the pixel and the sub pixel are equivalent. There is no contrast between the pixel and the sub pixel aside from that the "pixel" is the secret pixel in a secret picture, while the "sub pixel" is the pixel situated in shadows. In this manner, the shadow size is m times extended. The visual nature of a remade picture in VCS is debased by an enormous pixel extension, and in this way most investigations attempt to upgrade the visual quality or lessen the pixel development. Most VCSs shares one secret in particular, and this restricts its potential applications [8].

3. Proposed Methodology

Figure 1 shows block diagram of proposed frame work,Take any image which is to be shared secretly.the image is encrypted using AES utilizing a key given by the user and key generated by the genetic algorithm.the image is isolated in to N various shares utilizing K N secret sharing algorithm.these N shares can be circulated at the same time ,the end user needs just K of these shares to create the original image.the image is decrypted using pre-shared key and the key generated using genetic algorithm.Hence we will get the output image.

3.1 Advanced Encryption Standard

The AES has a data size 128 bits ie, 16 bytes with various key sizes of 128 bits, 192 bits and 256 bits. The key size is relies on the quantity of encryption rounds. For 128 bit key size it needs ten cycles, twelve cycles for 192 bits and fourteen for 256 bits. The 128 bit information is framed in 4X4 array which is called state array, is utilized in encryption process. The underlying information is changed over into state array during the encryption process, after each round this information is evolving until came into conclusive cipher text. During the decryption process, these cipher text arrays is continue changing to acquire original information.

3.2 K -N Secret Sharing Scheme

K -N Secret Sharing Scheme in which a secret is encoded into n shares with the goal that any k or on the other hand more offers can remake the mystery, while any k − 1 or then again less shares release no data about the secret. Rather than the customary cryptosystems, there exist SS plans whose decoding can be performed by people with no numerical calculations.

3.3 Genetic Algorithm

Genetic algorithms are a class of optimization algorithm [9], which finds the reasonable fittest solution for a given issue from a population. It depends on normal choice, inheritance, transformation, and hybrid. Change and hybrid are the hereditary calculation administrators in G.A. The genetic algorithm has a group of developmental calculations, alongside hereditary programming, development procedures, and developmental programming. Genetic algorithm finds a great deal of application in cryptanalysis field, arithmetic, building and so on. Population contains a few arrangements or people or chromosomes. Chromosome implies the conceivable answer for specific issue. When the underlying population is created, it enters the loop to produce new population. New population is created at the end of the loop. Contingent on the prerequisite the number of loops can be expanded to locate the fittest arrangement. Recovery process happens with the assistance of genetic algorithm operators. operators are chosen dependent on the application. After the generation of the underlying population, wellness of each individual is determined. In view of the aftereffect of the wellness estimation the best fittest arrangements are chosen from the population. These arrangements are taken as the guardians for the people to come. New posterity are created with the assistance of proliferation operators. It chooses at least two parents and after certain recombination new people are produced with genetic operators. Genetic algorithm is utilized rather than pseudorandom number generation on the grounds that, on account of pseudorandom number generator, it creates number that is by all accounts arbitrary yet as a matter of fact not. G.A is an improvement class and it creates number that is really arbitrary utilizing genetic operators. The wellness work in our execution of genetic algorithm likes chromosomes or people which have least relationship and most extreme contrast with other people of which have least connection and most extreme contrast with other people of a similar generation.

Genetic algorithm alongside installing is utilized in the proposed scheme to improve the security of the delicate data. Arbitrary keys are produced with the assistance of genetic algorithm. It creates interesting figure for same arrangement of plain text and key each time the calculation is completed. the irregular keys are made ceaselessly evolving. Our usage bolsters different synchronous occasions of the calculation. This calculation is reasonable for text, image and discourse record.

4. Result and Discussions

We experimented K-N sharing algorithm on finger print image. Figure 1 shows input image

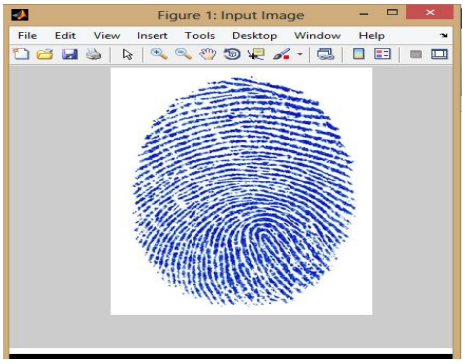

Figure 2: Input Image

Number of shares (n) = 3 Number of shares to be taken (k) = 2, The experimental result after encryption by the K-N encryption algorithm is given in the Figure 3.

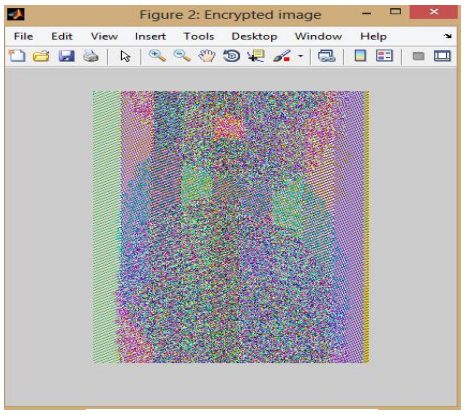

Figure 3: Encrypted image

We get the original image only by stacking k or more shares. If value of k is less than required (in this case k = 2), we will get a partial image.

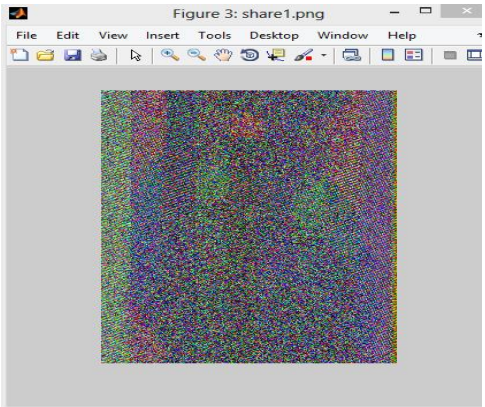

Figure 4: Share 1

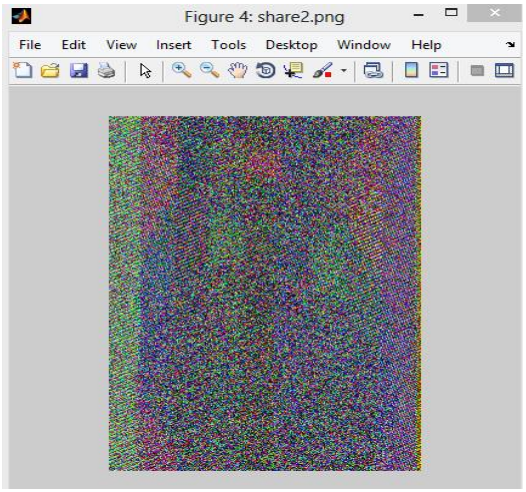

Figure 5: Share 2

After choosing any number of shares of all the generated shares, the reconstructed image is obtained and the shares generated is shown in Figure 4,5 and Figure 6 shows the reconstructed image

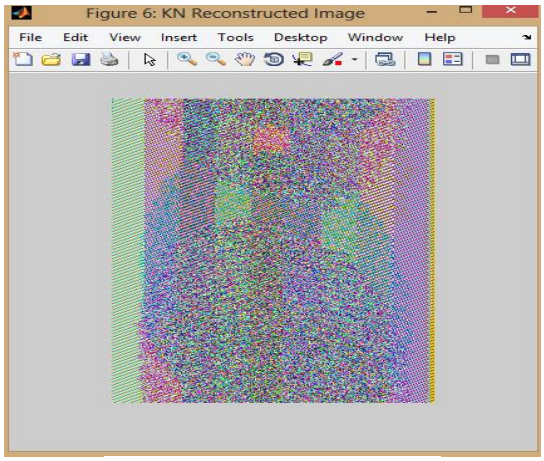

Figure 6: Reconstructed Image

Asymmetric key based encryption (AES encryption and genetic algorithm) at both the ends of KN Shares Algorithm is added to make the image more secure.

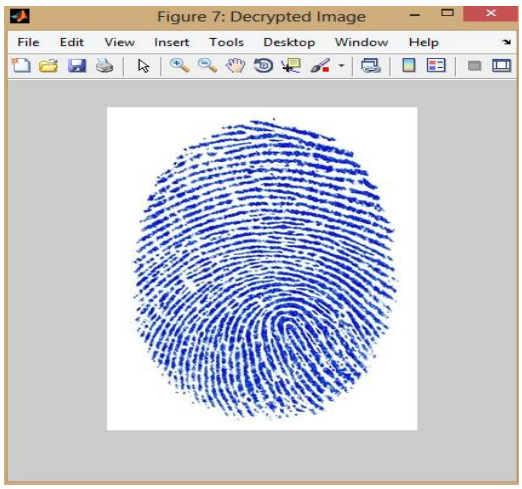

Figure 7: Decrypted image

The decryption result is shown in Figure 7. Thus, after encrypting the original image and then, regenerating the shares gives more better and noisy image. Now, the image will require at-least k shares along with the symmetric key generated by AES and genetic algorithm, in order to decrypt the image to its original form. Conveyed frameworks, suppose we have N distributed servers. Generally, in the event that we store a record in just a single server, there is a high hazard that in the event that it breaks or get hacked, the entirety of our information will be lost. So we might want to store our data in a dispersed way, with every server putting away a piece of the data. We can encode and break our information into N various parts with each part going into a server. Regardless of whether N − K servers are broken, we can at present produce our unique information utilizing the K alive server. Information move security is evident that moving our information through N channels is more secure than moving every last bit of it through one channel.

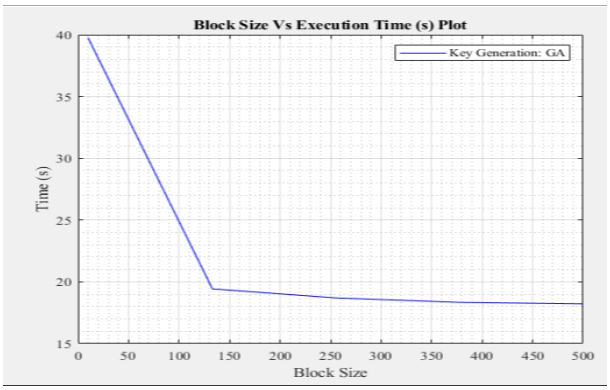

Figure 8: Block size Vs Execution time using GA

The overhead obtained for different block size and execution time are shown in the Figure 8. As the block size increases performance also increases. Genetic algorithm can be used for better security and high-performance applications.

5. Conclusion

This paper gives a brief idea about data transfer security. It clearly distinguishes the security of single server and distributed system. Secret Sharing is utilized to verify a secret in a conveyed manner, frequently to verify other encryption keys. The secret is part into different parts, called shares. These shares are utilized to recreate the original secret. Genetic Algorithm which is utilized to create key by the assistance of random number generator to make the key complex, thus giving an extra degree of security

References

[1] Manami Sasaki and Yodai Watanabe, “Visual Secret Sharing Schemes Encrypting Multiple Images,” ieee transactions on information forensics and security, vol. 13, no. 2, february 2018.
[2] Beimel and I. Orlov, “Secret sharing and non-Shannon information inequalities,” IEEE Trans. Inf. Theory, vol. 57, no. 9, pp. 5634–5649, Sep. 2011.
[3] Sindhuja K and Pramela Devi S, “A Symmetric KeEncryption Technique Using Genetic Algorithm,” IJCSIT.

[4] Ajay Kr. Phogat and Archana Das, "A Symmetric Cryptography Based on Extended Genetic Algorithm,"IJCTER, Volume 2 Issue 4, pp. 541-547, April 2016.
[5] Suvajit Dutta, Tanumay Das and Sharad Jash, "A Cryptography Algorithm Using the Operations of Genetic Algorithm & Pseudo Random Sequence GeneratingFunctions," IJACST, Volume 3, No. 5, May 2014.
[6] Rasul Enayatifar and Abdul Hanan Abdullah, "Image Security Via Genetic Algorithm," IPCSIT, Volume 14,2011.
[7] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography" Theor. Comput. Sci., vol. 250, nos. 1–2, pp. 143–161, 2001.
[8] C.-N. Yang and T.-H. Chung, "A general multi-secret visual cryptography scheme," Opt. Commun., vol. 283, no. 24, pp. 4949–4962, 2010.
[9] Aarti Soni and Suyash Agrawal," Using Genetic Algorithm for Symmetric Key Generation in Image Encryption," IJARCET, Volume 1 Issue 10, December2012.

Author Profile

Anu G S received the B.Tech degrees in Electronics and Communication Engineering from SHM Engineering College in 2017. During 2018-2020, she was doing her Master degree in Communication Engineering from APJ Abdul Kalam Technical University through MBC College Engineering and Technology.