IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10305

Multi-secret image sharing using the random image and Boolean operations

Sagar Mal Nitharwal[1], Pragya Chaudhary[2]

Assistant Professor, Computer Science, BTKIT Dwarahat, Almora, India[1]

Assistant Professor, Computer Science, BCE Bakhtiyapur, Patna, India[2]

Abstract: The sharing of personal information and private data via the Internet has increased exponentially, making it essential to protect data from unauthorized access. Numerous cryptographic techniques are used to provide data security, but these techniques have limitations and require encryption and decryption techniques with a high computation cost. To secure shared information, covert information exchange techniques have been proposed, but these schemes have high computational complexity, making them difficult to share. This paper discusses cryptographic techniques for encrypting and decrypting secrets that provide security for images transmitted over a network. In recent research, n secret images are shared among n or n+1 shared images, which poses a problem because fragmentary secret information can be reconstructed from n-1 or fewer shared images. In this paper, the proposed method employs random image and Boolean arithmetic to circumvent this issue. In this paper, we first generated n random images using the random image and XOR operation. Shared images are generated by applying XOR on random images in a sequence. This method assures that secret images cannot be reconstructed until all shared images are available.

Keywords: Pixel permutation, Secret image sharing, Random Image, Cryptography, Information sharing.

I. INTRODUCTION

In Information transmission over the internet is challenging and dangerous in a world that is becoming more and more digitalized as a result of pervasive internet usage. There is always a need for a trustworthy and safe transmission of information. It has been suggested to use a variety of techniques, such as data concealing, cryptography, and the sharing of secrets, to protect this digital data. Image secret sharing is the practice of sharing a secret image among participants or group members, with each person keeping only a section of the secret and each piece being useless for putting the original secret back together. Individual shares do not reveal the original secret; the original secret can only be recreated by combining a certain number of shares. This method of secret exchange takes into account computational expense and data storing security. Encryption and decryption rely on arithmetic and reasoning calculations. By dividing data into numerous pieces and storing them in different places, the risk of data loss and corruption can be decreased. Data transfer is now a crucial aspect of digital conversation. Secure communication is possible thanks to a variety of Internet apps. As a result, protecting information from unauthorized entry has emerged as a top priority. Data hiding methods have advanced as a result of this goal. The methods of steganography, watermarking, and cryptography are widely used to hide the initial message. Steganography modifies the characteristics of a cover work to reconstruct the original secret in order to hide a message inside another item. A well-known method for including information in a picture is digital watermarking. A receiver decodes ciphertext and converts it back to plaintext using a cryptography sender's encryption secret. A threshold access structure is presented by Reddy LS and Prasad MV [1] for the sharing of numerous secrets. A two-level coding technique is used for share generation from numerous secret images. In the first stage of encoding, secure Boolean procedures are used. At the second stage of encoding, Lagrange interpolation and the Chinese remainder theorem are both used. It is mainly helpful for the safe encryption of numerous secret images because it has two levels of encoding. It can recover private pictures without distorting them.

The capability to spread n private images to k shares is another benefit. In a k-threshold secret sharing scheme, a dealer who holds a secret s distributes pieces of this secret (the shares) to players; if k or more of these players pool their shares, they can determine s, but if fewer than k of them pool their shares, they cannot infer any information about s. This idea was put forth by Christian L. F. Corniaux and Hossein Ghodosi [2]. In 1979, Shamir presented a method that used polynomial interpolation in an endless field. Due to its elegance, simplicity, and information-theoretic security, this method is widely used in other cryptographic protocols. There are a few security proofs for the scheme, but none of them, as far as we are aware, are entirely dependent on Shannon's 1948 information-theoretic entropy function. We propose an analogous example. A technique for creating shares and disclosing secrets that relies on XOR operations and modular arithmetic is proposed by Maroti Deshmukh, Neeta Nain, and Mushtaq Ahmed [3]. To address the problems and shortcomings of existing authentication schemes, Ali A. Yassin, Abdullah A. Hussain, and Keyan Abdullah A. Mutlaq

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10305

[4] suggested a method that focuses on two-factor authentication and makes use of image partial encryption. They also used a fast partial image encryption method that adds symmetric encryption and Canny's edge detection as a second component. The edge pixels of the picture, which make up the bulk of the image's data, are encrypted in this scheme using the stream cypher, which is then used to authenticate legitimate users. Sunny Bhadlawala and Kajal Chachapara [5] put forth a structure that enables the creation of keys for particular users with particular access rights. A cloud user can create keys for numerous users with various entry rights to their files. AES and RSA are two examples of the cryptography algorithms used in this design. The safest cryptographic method is AES. When a key is created, the user (the person who created the key for their own files) has the option of giving it to any other user they choose (user for whom key is generated). Therefore, the owner-specified permission will be given when a determined user tries to access cloud-based files using that key. This limited user access is safer than giving out the user's passcode. In a manner similar to how cloud users can create a key for a particular file, user, and authorization, cloud service providers can also introduce the idea of designating files. Then, these keys can be given out to different users. Sagar In their framework, proposed by Mal Nitharwal and Harsh Verma [6], random images are produced using an encryption algorithm, the first random image is generated by XORing secret images, and subsequent random images are generated by using the encryption algorithm on the first random image. Secret images are XORed with random images in a specific sequence to create shared images. In general, the papers discussed above are susceptible to brute force attacks and chosen plaintext attacks, as well as having a high computational complexity that results in longer computation times to create and recover shared and secret images. To address these limitations, our proposed method ensures that secret images cannot be recovered until all shared images are available, and it significantly reduces the time required for calculating shared images and recovering secret images through the use of a simple XOR operation and transpose.

II. METHODS AND MATERIALS

Proposed Method: We suggested a method for the protected and multi-secret sharing of images based on Boolean operations and random images. The first random image is generated using values between 0 to 255. Using this random image, the XOR operation is performed on both the secret images and the random image, which results in the generation of n-1 additional noise pictures. The proposed method generates a random image by using a random function. After generating the first random image, the remaining n-1 random images are generated by XORing the first n-1 secret images with the first random image. After generating random shared images are generated as the first shared image is the same as the first random image, a second random image is the same is the second random image and rest of the images are generated by XORing two successive random images as shown in the algorithm given below.

Algorithm: Proposed Sharing Procedure.
Input: n secret images {I1, I2 ⋯ In}.
Output: n + 1 shared images {S1, S2 ⋯ Sn+1}.
1. Generate a Random image
T= random (0, 255)
2. Compute n − 1 random matrices {B1, B2 ⋯ Bn−1} using XOR operation
Bi = Ii ⊕ Y where {i = 1, 2, ⋯ , n − 1}
3. Generate shared images
S1 = T
S2 = B1
Si = Bi-1 ⊕ Bi−2, where {i = 3, 4, ⋯ , n}
Sn+1 = I1 ⊕ Bn−1

Proposed Recovery Procedure: In this proposed secret image sharing method, secret images are recovered by XORing all the shared images, this operation retrieves the first shared image(B1) same as the proposed sharing method. Rest of the random images (Bi, i=1 to n) are generated by XORing previous random image (Bi-1) and next shared image (Si+1).
Input: n+1 shared images {S1, S2 ⋯ Sn+1}.
Output: n Recovered images {R1, R2 ⋯ Rn}.

1. Generate first random image by XORing all secret images
B1= S1⊕ S2⊕ ⋯ ⊕ Sn⊕ Sn+1
2.Compute remaining n-1 random matrices {B2 ⋯ Bn−1} using XOR operation
Bi = Bi-1 ⊕ Si+1 where {i = 2, ⋯ , n − 1}
3.Generate recovered images
Ri = Bi ⊕ S1 where {i = 1, 4, ⋯ , n}

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10305

III. RESULTS AND DISCUSSIONS

In this section, we describe the findings of our experiments and our analysis of the (n, n+1)-MSIS method that we suggested. MATLAB 18 is used to conduct all of the investigations on a computer with an Intel(R) CPU running at 2.50 GHz and 4 GB of Memory. The (n, n+1)-MSIS scheme technique that was proposed works exceptionally well with both binary and grayscale pictures. The dimensions of each monochrome and binary picture are respectively 256X256. We have only captured grayscale images for our experimental research.

Experimental Results Fig. 1 shows the experimental results of sharing three secret images of size 256 × 256. Fig. 1(a)-(c) shows three secret images: Lena, Baboon, and Cameraman. Fig. 1(d)-(f) shows three shared images. Fig. 1(g)-(i) shows recovered secret images, the same as the original secret images.

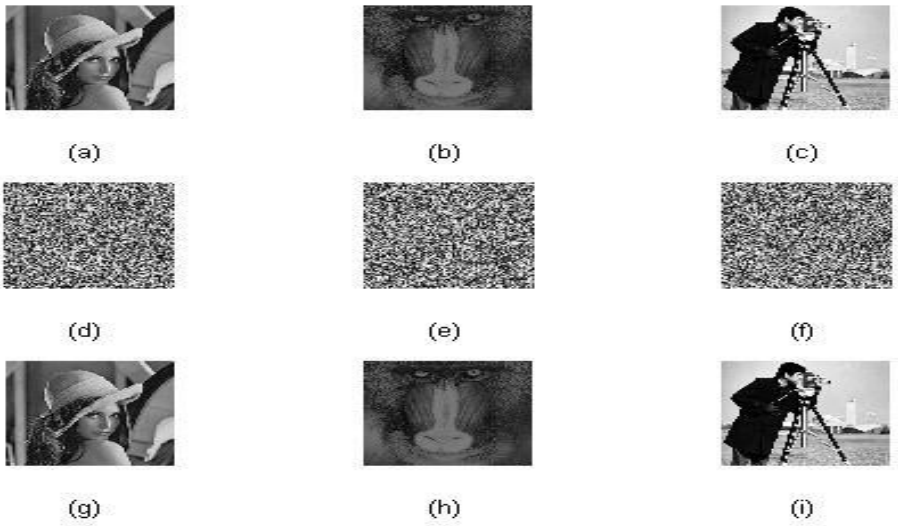

Fig 1. Three secret image-sharing examples: (a-c) Secret images, (d-f) shared images, (g-i) Recovered Images

For Statistical analysis, we have used correlation and Root Mean Square Error to match hidden images and restored images of the proposed (n, n+1)-MSIS method for quantitative analysis. The correlation is +1 to -1. +1 means the hidden and recovered photos are the same, and -1 means opposite or inversely linked. Comparison is shown in the table given below correlation of shared and recovered images is 1, and RMSE is o which shows that shared and recovered images are same.

$$Correlation = \frac{N\sum XY - (\sum X)(\sum Y)}{\sqrt{(N\sum X^2 - (\sum X)^2)(N\sum Y^2 - (\sum Y)^2)}}$$

where N is: Number of pairs of scores, XY is: Sum of products of paired scores, X is: Sum of X scores, Y is: Sum of Y scores, X^2 is: Sum of squared X scores, and Y^2 is: Sum of squared Y scores

Table: Matching between secret and recovered images using correlation and RMSE technique

Secret and Recovered images Correlation RMSE	Correlation	RMSE
I1, R1	1.00	0
I2, R2	1.00	0
I3, R3	1.00	0

IV. CONCLUSION

This paper presents a safe (n, n+1)-multi-secret picture-sharing system. This research uses a random image and Boolean XOR operation to share n secret images among n+1 shared images. This scheme generates the random image using a random function containing pixel values between 0 to 255. This technique conquers the limitations of previous methods, like reducing time complexity and increasing the security of shared images. Statistical analysis results show that the

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IARJSET.2023.10305

shared image pixel distribution is consistent, and the relationship among the shared and recovered image PSNR is infinite, which shows that shared and recovered images are the same. Future development of this work may investigate using a two-dimensional image at the bit level to achieve a high level of security.

REFERENCES

[1]. Reddy LS, Prasad MV. Multi-secret sharing threshold access structure. In2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI) 2015 Aug 10 (pp. 1585-1590). IEEE.

[2]. Corniaux CL, Ghodosi H. An entropy-based demonstration of the security of Shamir's secret sharing scheme. In2014 International Conference on Information Science, Electronics and Electrical Engineering 2014 Apr 26 (Vol. 1, pp. 46-48). IEEE.

[3]. Deshmukh M, Nain N, Ahmed M. An (n, n)-multi secret image sharing scheme using boolean XOR and modular arithmetic. In2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA) 2016 Mar 23 (pp. 690-697). IEEE.

[4]. Guo T, Liu F, Wu C. K out of k extended visual cryptography scheme by random grids. Signal processing. 2014 Jan 1;94:90-101.

[5[. Deshmukh M, Prasad MV. Comparative study of visual secret sharing schemes to protect iris image. International Conference on Image and Signal Processing (ICISP) 2014 (pp. 91-98).

[6]. Nitharwal SM, Verma HK. A Boolean-based multi-secret image sharing scheme using bit-reversal. In2017 International Conference on Intelligent Communication and Computational Techniques (ICCT) 2017 Dec 22 (pp. 114-118). IEEE.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License