IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907077 |

Security of Confidential Data using Secure Server using Share Generation Scheme

Anuja Dattatray Yadav[1], Prof. Gopal Chandangole[2]

ME Student, Zeal College of Engineering and Research, Pune, Maharashtra, India [1]

Professor, Zeal College of Engineering and Research, Pune, Maharashtra, India [2]

ABSTRACT: Security has become an inseparable issue as internet is ruling the world. Every day we are doing various activities such as e-banking, e-shopping or information transfer through internet so there exists a need for safe and secure transactions. Extended visual cryptography is very advanced technique for providing security to information which will be going to transfer through network. In this paper, we exploit extended visual cryptography technique for military application security. Without sending password directly as it is from sender to receiver we are going to create shares of password and those shares will be transfer through secure server to receiver. When receiver will combine this shares then only complete password will be revealed. In this paper we provide overview of extended visual cryptography and Algorithms implementation is presented in this paper for share generation of password.

KEYWORDS: Steganography, Cryptography, Extended Visual Cryptography, Secure Server, and Share Generation.

I. INTRODUCTION

1.1 Background:

We are in 21st century and everything is digitalized. Lot of activities done through internet. Everyday huge transaction takes place through cloud so that tremendous amount of data gets generated. Handling such amount of data is not an easy task. There are various techniques, algorithms and software for handling such type of heterogeneous data. While transferring the data through network from sender to receiver integrity need to be maintained. Security is always main issue while transferring confidential data through network. There are various techniques and softwares that helps to provide security to confidential data but attackers are smart enough to reveal the original data. So there is always requirement of more and more advanced technique to deal with various attacks. The attacks are either active or passive. Active attacks are those which modify the data that is passing through network while passive attack is the attack which only monitors network. Traditional password conversion scheme uses hash values. But this scheme is easy and simple to crack. There are various password cracking tools and password cracking websites. Many people use short length of passwords in multiple systems and are neglectful password management. Con- sequentially cyber accidents are occurred often. In today's world online transaction has become very common. There are various attacks present during the online transaction. Phishing is a very common attack. In phishing process, suppose cheater sends out thousands of phishing emails with a link to the fake website. Victims click on links in email believing it is legitimate. They enter personal information on that fake website. Fraudsters collect the stolen data and login into correct website. This is an overall process of phishing.

For providing security to confidential data various data hiding techniques are being introduced.
Steganography, Watermarking, Cryptography are some of the data hiding techniques. These techniques have various drawbacks. In case of watermarking receiver is not able to easily extract the original information. Steganography is hiding data under another data. Problem with steganography is that there are overcomes drawback of steganography by using key for security of data. But in this case security of key is main concern. There are various applications where encryption, cryptography is used. Advanced Encryption Standard is the standard algorithm used for the encryption is considered as one of the strongest algorithm. Its block size and lengthy key size make it most effective scheme for the encryption. It falls under the category of the symmetric key encryption in which both the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907077 |

communicating parties uses same key. It encrypts and decrypts a data block of 128 bits. The key size, in which can be 128, 192 or 256 bits. It uses 10,12or 14 rounds depending on the key size.

A basic model of VC was proposed by Naor and Shamir, where a secret image is encrypted into several shares by using two basic matrices. To decrypt the secret, sufficient shares are printed on the transparencies and stacked together. The stacking operation can be simulated by the OR operation, as a result, the conventional VC is referred as OR-based VC. Based on the pioneer work of Naor and Shamir, many issues on OR-based VC scheme have been extensively studied, such as the meaningless share.

Generation Extended visual cryptography is an extension to visual cryptography. It helps to encrypt the various formats of data in secure way by generating shares. But decoding never requires any computations. By using human visual system we can decrypt any encrypted data.
Flow of extended visual cryptography consists of three phases that is confidential data, share splitting phase and combination phase etc. Confidential data is data that need to be transfer securely through network. That data may consist of confidential text, image etc. Which need to maintain securely. Without directly transferring it towards receiver it is forwarded to second phase. Then pass- word is divided into encrypted shares. Then those shares will be transmitted towards receiver. In third phase those share will combine and reveal the confidential data.

1.2 Objectives:
1. To enhance the security of confidential data.
2. To improve the performance of system by using multiple layers of security.
3. To maintain integrity of confidential data.
4. To perform the decryption by human visual system for extended visual cryptography.

1.3 Problem Statement:
Design a system for security of confidential data using secure server that generate shares of that confidential data and individual shares will not reveal any data.

II. LITERATURE SURVEY

1. Long Bao, Shuang Yi and Yicong Zhou [1] Secret image sharing is an interesting researchtopic in multimedia security society. Its function is to encrypt an original image inton different shares. Using k (k n) or more shares can successfully reconstruct the originalimage. With less than k shares, any information of the original image cannot be accessed.This unique and interesting function allows secret image sharing to be used in many fieldssuch as general access structure, discrete memorials network, visual authentication and identification, data sharing, and so on.

2. Dana Yang,InshilDoh ,kijoonChae [2] this paper proposes the concept of visual cryptographyand optical character recognition. In existing system password is converted intohash values but it is easily hack able. It also shows the negative behavior while setting thepassword. Visual cryptography is share generation scheme proposed by Naor and Shamir in1994.This paper represents survey result of password management.

3. ShubhangiKhairnar,ReenaKharat [3] this paper presents security related techniquesin on- line transaction application. Everyday number transactions takes place so there arechances of phishing attacks. This paper provides the security from phishing attack by using visual cryptography of QR code. This paper uses OTP for phishing website detection.Encryption is done by covering OTP with QR code and then share generation will be takesplace.

4. Mohitrajput ,Marotideshmukh , Neeta nain[4] this paper presents various data hidingtechniques such as watermarking, steganography and cryptography. Secret sharing conceptis used to provide best security. Stenography is used to hide secret image into cover image.The pro- posed scheme used n cover images to provide randomness to n + 1 shared imagesso that less than n + 1 shares can't reveal any information of cover images and the secret image.Stacking of less than n recovered cover image with steno image does not reveal secretimage.

5. Shankar K, Eswaran [5] this paper shows modern public key cryptography. Factorsdecomposition hassles dependent on huge numbers are habitually employed, the classic examplebeing the RSA cryptography. In visual cryptographically

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907077 |

the generated image sharesare encrypted by using RSA algorithm. The combination of visual cryptography with thepublic key encryption ends in high security while transmitting the image.

6. Xiaotin Wu and Wei Sun[6] this paper presents concept of probabilistic visual cryptography.
In that frequency of white pixel used to determine contrast of recovered image.Disadvantage of this method is that it always requires enough white pixels inside recoveredimage.

7. Duanhao Ou, Wei sun, Xiaotian Wu [7] A basic model of VC was proposed by Naor andShamir , where a secret image is encrypted into several shares by using two basic matrices.To decrypt the secret, sufficient shares are printed on the transparencies and stacked together.The stacking operation can be simulated by the OR operation, as a result, the conventionalVC is referred as OR-basedVC. Based on the pioneer work of Naor and Shamir, many issueson OR-based VC scheme have been extensively studied, such as the meaningless share.

8. Soumya S. Hegde, Bhaskara Rao N [8] this paper shows the concept of OR based visualcryptography. This technique performs computation free decoding. But visual qualityof recovered image is poor. This technique does not provide strong security.

9. Chingnung yang, Li zhe sun, Song rueicai [9] this paper present the Region incrementing visual cryptography technique. This technique maintains multiple level of secrecy inside one image. Contents will be encoded in multiple regions associated with secret levels.

10. Song wan, Yulianglu ,Xuehuyan and lintaoliu[10] this paper presents the idea about visual cryptography and flaws about it. Collection of white and black pixel is share. Even human visual system is able to recognize the secret data when these pixels are printed close to each other. Problem with visual cryptography is pixel expansion and poor image quality.

III. PROPOSED SYSTEM ARCHITECTURE

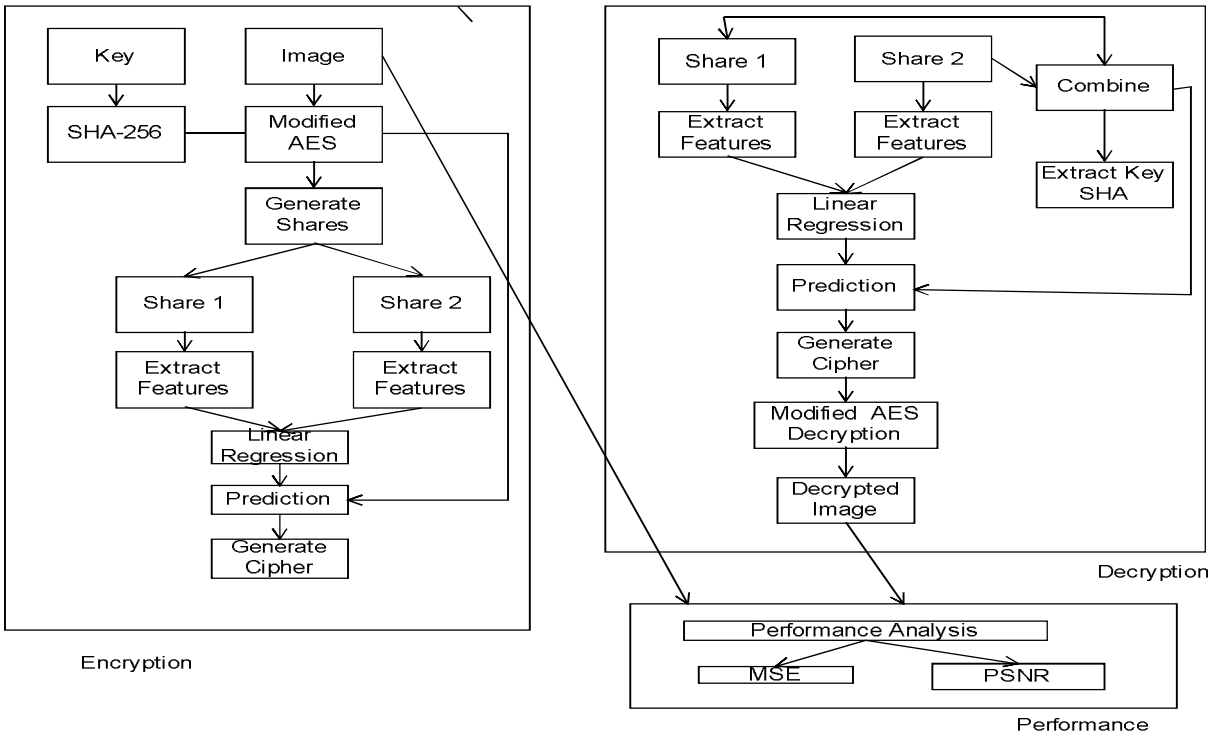

Figure: System Architecture

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907077 |

In Visual Cryptography, there are some algorithms for encryption and decryption of images. In this Project we are using one secret image and two cover images, and these images are overlapped with each other so that the secret image is secured in the two cover images. So if these two cover images are simultaneously available then only we can access the secret image. The single share can't give any information of the secret image. In our proposed system, we are using SHA-256 algorithm and linear regression algorithm. In encryption method, we are using SHA-256 algorithm. Shares will get generated from the images. Features will be extracted from the two generated shares.Once shares generated linear regression is applied and cipher get generate.
In decryption, Share will be combined with the help of linear regression. Key will get extracted with SHA. From the generated shares, predicted result will show and cipher will get generate. On generated cipher modified AES decryption is applied and image get decrypted. Performance analysis done – MSE & PSNR

IV. METHODOLOGY

Algorithms used:

1. **SHA-256:**

- SHA-256 is one of the most secure hashing functions on the market. The US government requires its agencies to protect certain sensitive information using SHA-256. While the exact details of how SHA-256 works are classified, we know that it is built with a Merkle-Damgård structure derived from a one-way compression function itself created with the Davies-Meyer structure from a specialized block cipher.
- Three properties make SHA-256 this secure. First, it is almost impossible to reconstruct the initial data from the hash value. A brute-force attack would need to make 256 attempts to generate the initial data. Second, having two messages with the same hash value (called a collision) is extremely unlikely. With 2 256 possible hash values (more than the number of atoms in the known universe), the likelihood of two being the same is infinitesimally, unimaginably small.
- Finally, a minor change to the original data alters the hash value so much that it's not apparent the new hash value is derived from similar data; this is known as the avalanche effect.
- SHA-256 is used in some of the most popular authentication and encryption protocols, including SSL, TLS, IPsec, SSH, and PGP. In UNIX and Linux, SHA-256 is used for secure password hashing. Crypto currencies such as Bit coin use SHA-256 for verifying transactions.

2. **Linear Regression:**

- Linear Regression Algorithm is a machine learning algorithm based on supervised learning.
- Linear regression is one of the very basic forms of machine learning where we train a model to predict the behavior of your data based on some variables. In the case of linear regression as you can see the name suggests linear that means the two variables which are on the x-axis and y-axis should be linearly correlated.

3. **AES Algorithm:**

- AES was built to secure government in various fields.
- The AES algorithm is designed to use minimal cipher blocks from 128-bit input blocks and supports 3-key-sizes, namely 128 bit, 192 bit, and 256-bit keys.
- The encryption process in the AES algorithm consists of 4 types of bytes transformation, namely Sub-Bytes, Shift Rows, Mix columns, and Add Round Key.
- At the beginning of the encryption process, the input that has been copied into the state will undergo a byte transformation Add Round Key. After that, the state will undergo repeated Sub-Bytes, Shift Rows, Mix Columns, and Add Round Key transformations as much as Nr.
- This process in the AES algorithm is called a round function. The last round is somewhat different from the previous round-round wherein the last round, the state does not undergo Mix Columns transformation.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907077 |

V. RESULT

As per our proposed system, we got the following result. System Screenshot attached.

Figure: Sign Up Screen

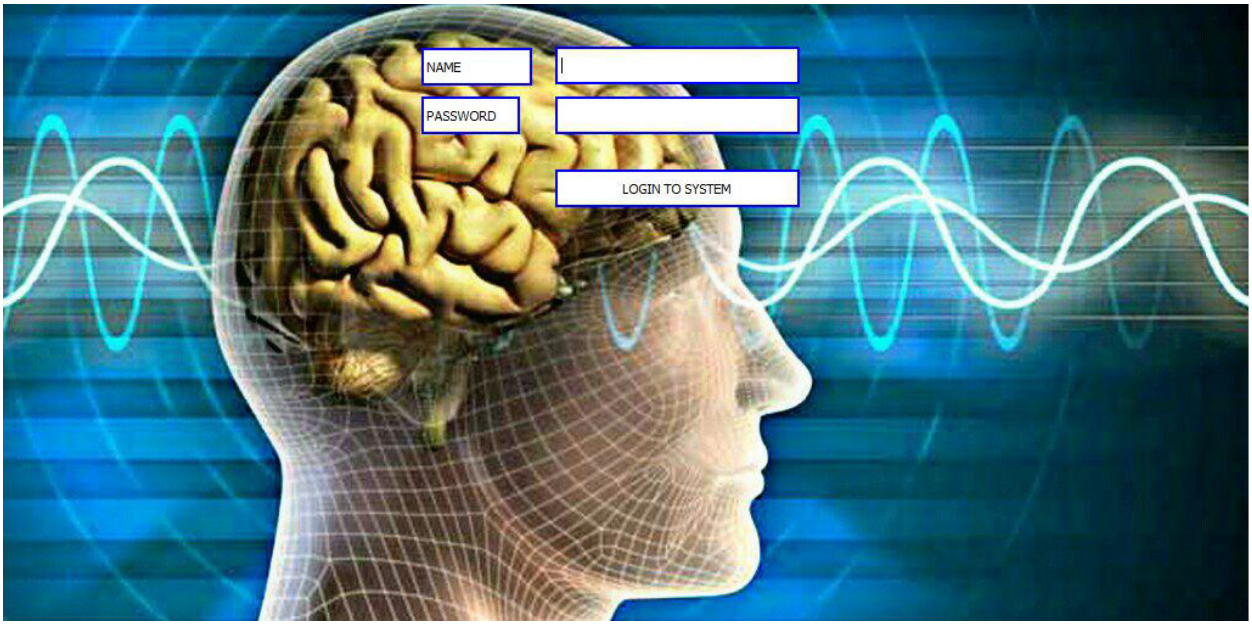

Figure: Login Screen

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907077 |

Figure: Share 1

Figure: Share 2

VI. CONCLUSION

We proposed system for Security using extended visual cryptography. Using extended visual cryptography we can verify the shares are genuine or not. Therefore, it provides better security in preventing phishing attack compared to other techniques. This technique is less time consuming because crypto encryption and decryption takes place at secure server side.In future extended visual cryptography is applied on video.

FUTURE WORK

In future we will extend this system performance to improve security of data which is in the form of video.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907077 |

REFERENCES

[1]Long Bao, Shuang Yi and Yicong Zhou, Combination of sharing matrix and image encryption for lossless (k, n) secret image sharing,IEEE 2016

[2] Dana Yang,InshilDoh ,kijoonChae, Enhanced password processing scheme based on visual cryptography and ocr,IEEE 2017.

[3] ShubhangiKhairnar,ReenaKharat, Online fraud transaction prevention system using extended visual cryptography and QR code,IEEE 2016.

[4] Mohitrajput, Marotideshmukh , Neeta nain, A novel approach for concealing image by utilizing the concept of secret sharing scheme and steganography, IEEE 2016.

[5] Shankar K, Eswaran P, Sharing a secret image with encapsulated shares in visual cryptography, Science Direct 2015.

[6] Xiaotin Wu and Wei Sun, Extended capabilities for XOR based visual cryptography, IEEE 2014.

[7] Duanhao Ou, Wei sun, Xiaotian Wu, Non expansible XOR based visual cryptography scheme with meaningful shares,Elsevier 2015.

[8] Chingnung yang, Yao yu yang, new extended visual cryptography schemes with clearer shadow images, Elsevier 2014.

[9] Soumya S. Hegde, Bhaskara Rao N, Cloud security with visual cryptography, IEEE Publication 2016.

[10] Chingnung yang, Li zhe sun, Song rueicai, Extended color visual cryptography for black and white secret image, Science direct 2016.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details