ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

Survey on Online Transaction using Visual Cryptography and Steganography

S.D Gaikwad[1], Anshika Kulshreshtha[2], Pooja Nagar[2], Sukirti Misri[2]

Asst. Professor, Dept. of I.T., JSPM's BSIOTR, Pune, Savitribai Phule Pune University, Maharashtra, India[1]

B. E Student, Dept. of I.T., JSPM's BSIOTR, Pune, Savitribai Phule Pune University, Maharashtra, India[2]

ABSTRACT: In this paper,we are going to see a very smart system for recognizing persons in various conditions. This paper, proposes a recognition system by using different algorithm techniques. We are using R-Cascade, PCA (Principle Component Analysis), FJ-RC4 algorithms for building this system. The main goal of this system is to identify bank account holders at each transaction. Most probably we use this system in public places where we can monitor and identify bank account holders. In this digital world as everywhere computerized systems are working, we are taken initiative to help the Banks and its Users by increasing security at one step ahead. Smart System Person Recognition system is the improvement that has taken place in field of identifying and locating Bank Account Holders while doing the transactions.

The designed system is used to transmit information about bank account holders which are identified by centralized Bank database. In this system we make some modules which are well compacted in a software. Cameras placed while doing the transactions online or in ATM are managed by DVR system and this DVR system can be access through internet anywhere anytime. So, at server side means in bank we make a web application and by using this web application we fetch live recording of cameras and matches this recording with users database which is already exists on server application. If any person matches with the database then user can easily get done their transactions.

KEYWORDS: Criminal identification, FJ-RC4, IR Cameras, PCA, Haar Cascade, Steganography and Visual Cryptography.

I. INTRODUCTION

STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY: - Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Text, image, video, audio are used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line, in open spaces, in word sequence. Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication.

Visual Cryptography (VC), proposed by Naor et al. in, is a cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over an untrusted communication channel. Only combining the k shares or more give the original secret image.

FJ-RC4:

The new developed approach based on the RC4 for the purpose to making strong the RC4 approach against the attacks. In this study shows the new KSA stage of the RC4 having vulnerable stage against the attack so in this study introduced new approach named as FJ-RC4 on the bases of the new developed KSA algorithm to making strong the stage against the attacks and also to the RC4 stream cipher. In this self developed new algorithm, FJ-RC4 is built from the new KSA, which uses the key stream in three stages process and shares the PRGA structure same as based on the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

previous structure of the PRGA of RC4, just one difference in PRGA stage of the FJ-RC4 algorithm, it is three stages encryption and decryption process but in the PRGA of RC4 having one stage encryption and decryption process.

II. LITERATURE SURVEY

Title 1: Review Of Steganography Research And Development

Authors: Latika, Yogita Gulati

Year of Publication: 2015

Providing confidential information and establishing concealed association has been a great interest since long time ago. Steganography is the art and science of hiding a secret message in a cover media such as image, text, signals or sound in such a way that no one, except the intended recipient knows the existence of the data[1]. Steganography combined with encryption will be a powerful and efficient tool that provides high level of security.

Title 2: A New Image Steganography Technique Based On Similarity In Secret Message

Authors: Kumar, R. And Chand, S.

Year of Publication: 2013

In this paper [2], we propose a new image steganography scheme for coloured images based on the cluster analysis. In this scheme, we analyze the secret data in order to make its clusters. The secret data can be textual, image/video or audio/speech. We then calculate the difference value between the secret data and the minimum value contained in the cluster. We do not hide actual secret data; the difference value is embedded equally into two channels of the image. The experimental results show that our proposed method has enhanced security as compared to the modified Kekre algorithm and pixel intensity based high capacity data embedding method. Furthermore, our scheme has good hiding capacity, high PSNR value, and very low MSE value.

Title 3: A New Approach To Hide Text In Images Using Steganography

Authors: Vipul Sharma and Sunny Kumar

Year of Publication: 2013

In this paper [3], we have proposed a new steganographic algorithm that is used to hide text file inside an image. In order to increase/ maximize the storage capacity we have used a compression algorithm that compresses the data to be embedded. Before the hiding process, the sender must select an appropriate message carrier, an effective message to be hidden as well as a secret key used as a password. A robust steganographic algorithm must be selected that should be able to encrypt the message more effectively. The sender then may send the hidden message to the receiver by using any of the modern communication techniques. The receiver after receiving the message decrypts the hidden message using the extraction algorithm and a secret key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

III. PROPOSED ALGORITHM

THE FJ RC4 ALGORITHM

Key Schedule Algorithm

The key mechanism in FJ-RC4 is very similar to one that used in RC4, with the distinction that Key needs to be initialized as well as Algorithm / Pseudo code. The core of RC4 algorithm remains the same in our algorithm. It means the encryption and decryption phases are the same as RC4 which is simple and fast. However, to prevent attacks which are happening through key scheduling, we made a strong algorithm for KSA. In FJ-RC4 at beginning of the process the main key is divided by three equal portions to make three different sub-keys. If the length of main key is not divisible by three, then we use zero padding to make it divisible by three.

```
String key;
String[] array = new String[3];
int remain = 3 - (key.length() % 3);
if(remain != 3) {
for(int i=0;i<remain;i++) {
key = key + "0";
Repeating 0 as necessary.
}
}
int temp = key.length() / 3;
array[0] = key.substring(0, temp);
Fill the first array.
array[1] = key.substring(temp, temp+temp);
Fill another array of the same size with the key
array[2] = key.substring(temp+temp, key.length());
```

Fill third array of the same size with the key. In the FJRC4 the string message that is supposed to be locked for the encryption will be combined with the first sub-key array, array[0], using bit-wise Exclusive OR for the first stage of encryption process. The result from this step will be combined with the second sub-key array, array[1], using bitwise Exclusive OR for the second stage of encryption process. Finally, the result from step 2 will be combined with the third sub-array,array[2] ,using bit-wise Exclusive OR for the third stage of encryption. The third encryption process will produce the cipher string by the FJ-RC4.

Decryptions

It should be mentioned that bit-wise Exclusive OR operation has symmetric property and original string can be

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

s

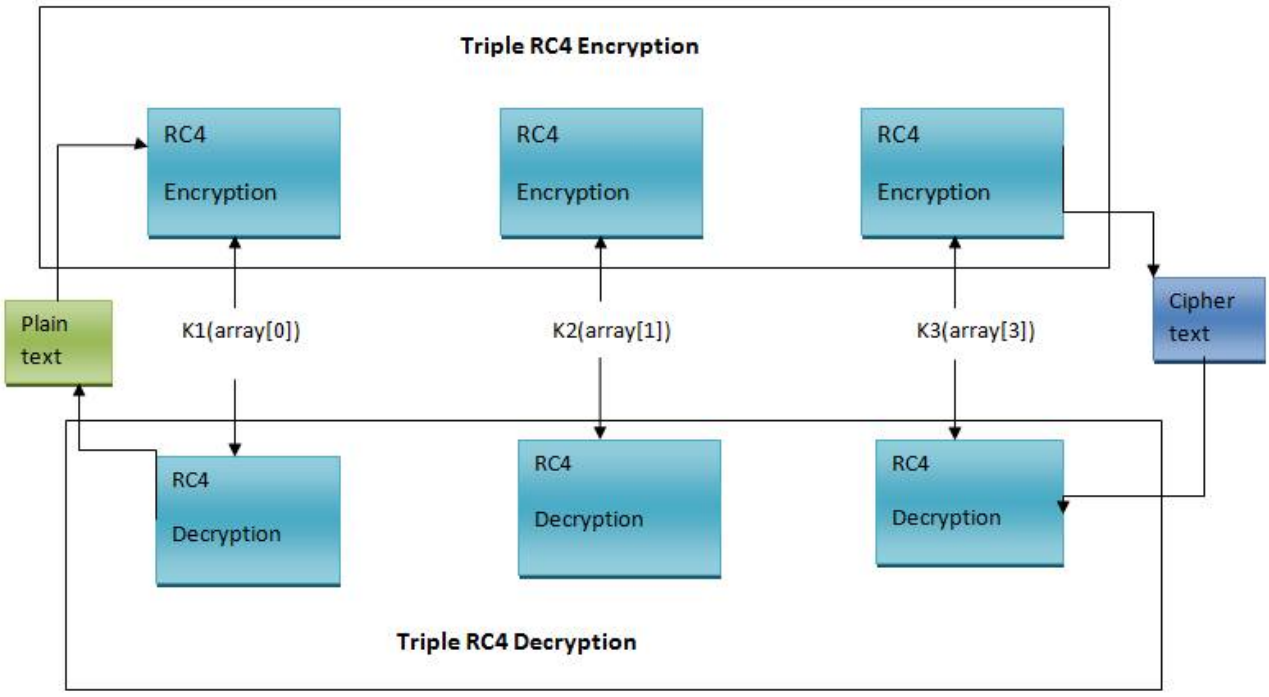

Fig: The Encryption And Decryption Algorithm

recovered from the encrypted string using the cipher string that has been encrypted by FJ-RC4. Since the main key is divided by three portions during the encryption process, thus the decryption process is in the opposite direction of the encryption process. First, the cipher string must be combined with the third sub-key array using bit-wise Exclusive OR for the first stage of decryption. The result from this step will be combined with the second sub key array using bit-wise Exclusive OR for the second stage of decryption. Finally, the result from step 2 will be combined with the third sub-array, using bit-wise Exclusive OR for the third stage of decryption. Thus, third decryption process will produce the original string by the FJ-RC4. .The Encryption And Decryption Algorithm is shown in Fig.

IV. PSEUDO CODE

Algorithm PCA

The PCA algorithm consists of 5 steps:

1. Subtract the mean: subtract the mean from each of the data dimensions. The mean subtracted is the average across each dimension. This produces a data set whose mean is zero.
2. Calculate the covariance matrix:

   $$C^{n\times n} = (c_{i,j}, c_{i,j} = cov(Dim_i, Dim_j))$$

   Where $C^{n\times n}$ is a matrix which each entry is the result of calculating the covariance between two separate dimensions.

3. Calculate the eigenvectors and eigen values of the covariance matrix.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website:www.ijircce.com

Vol. 5, Issue 2, February 2017

4. Choose components and form a feature vector: once eigenvectors are found from the covariance matrix, the next step is to order them by eigen value, highest to lowest. So that the components are sorted in order of significance. The number of eigenvectors that you choose will be the number of dimensions of the new data set. The objective of this step is to construct a feature vector (matrix of vectors). From the list of eigenvectors take the eigenvectors selected and form a matrix with them in the columns:

   FeatureVector = (eig_1, eig_2, ..., eig_n)

5. Derive the new data set. Take the transpose of the FeatureVector and multiply it on the left of the original data set, transposed:

   FinalData = RowFeatureVector x RowDataAdjusted

   Where RowFeatureVector is the matrix with the eigenvectors in the columns transposed (the eigenvectors are now in the rows and the most significant are in the top) and RowDataAdjusted is the mean-adjusted data transposed (the data items are in each column, with each row holding a separate dimension).

V. CONCLUSION

This paper presented a smart system for person recognition which is a best solution for account holder identification. By using this system Banks working will be somehow simplify. The successful solution for person recognition is achieved by this system. By using this system user's database is centrally managed and used for systematic identification of users.

REFERENCES

1. Latika, Yogita Gulati, "Review Of Steganography Research And Development", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume – 5 Issue-04 , 2015.
2. Kumar, R. And Chand, S., "A New Image Steganography Technique Based On Similarity In Secret Message", Confluence 2013: The next generation Information Technology Summit(4th International Conference),2013.
3. Vipul Sharma and Sunny Kumar," A New Approach To Hide Text In Images Using Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 4, April 2013.
4. Dagar, S. "Highly randomized image steganography using secret keys" .Recent Advances and Innovations in Engineering (ICRAIE), Volume-9 Issue-04, s May 2014.
5. Siddharth Singh and Tanveer J. Siddiqui "A Security Enhanced Robust Steganography Algorithm for Data Hiding" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.
6. T. Morkel , J.H.P. Eloff and M.S. Olivier "An Overview of Image Steganography".
7. N Ghoshal, J K Mandal ,"Steganographic scheme for colour image authentication (SSCIA)", Recent Trends in Information Technology ICRTIT 2011 International Conference, 2011.
8. Mr.Dilip Bahadur Malla, Ch.Dayakar Reddy, "Secure Online Payment System Using Cryptography Techniques",IJMETMR,2016.