IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 3, March 2017

Visual Cryptography for Authentication and File Sharing using different techniques in Web Portals

Pankaj Sonune[1], Sourav Sengupta[2], Shikhar Srivastava[3], Tushar Sonawane[4]

Student, Computer Department, Smt. Kashibai Navale College of Engineering, Pune-411041, India [1,2,3,4]

Abstract: For security purposes every application provides user authentication. In user authentication the process which we have to pass through is username and password. Authentication process divided into Token based authentication, Biometric based authentication and Knowledge based authentication. Most of the web application provides knowledge based authentication which include alphanumeric password as well as graphical password. In today's changing world when we are having number of networks and personal accounts some sort of easy authentication scheme needs to be provided. In this we provide the image based authentication that can do login. Password image is generated and it will be downloaded from the email which is stored at the time of registration. Every time the image will be unique. In this system the OTP based authentication is also used. In this system the data file that will be transferred within this web portal will be embedded using image as key into the video file and sender sends this file to the receiver and the receiver extracts the data file by using the image as a key.

Keywords: Visual Cryptography, Encryption/Decryption, Steganography, DCT, K-N Algorithm, Watermarking, AES Algorithm.

I. INTRODUCTION

Visual cryptography technique allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. Security has become an inseparable issue as Information Technology is ruling the world now. Cryptography in the study of mathematical techniques related aspects of information security such as confidentialities, data security, entity authentication, but it is not only the means of providing information security, rather one of the techniques. Visual cryptography can be applied for copy right for images, access control to user images ,visual authentication and identification any kind images of images like(normal or digital).

Visual cryptography is a new technique which provides information security which user simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. Visual Cryptography is a secret sharing scheme which can be used to share secrets among participants who do not have the knowledge of complex mathematics.

Any written printed text, pictures etc. can be encrypted using Visual Cryptography and the decryption is done based on the human visual sensibility. The secret is segregated into n parts in the encryption process, each known as 'shares'. The required numbers of shares are then superimposed in a correct alignment to reveal the secret in the decryption process. The advantage of using Visual Cryptography over traditional cryptographic techniques is that the former requires no complex mathematical ability for the decryption of the secret message.

1. VISUAL CRYPTOGRAPHY FOR SECURE AUTHENTICATION –

In previous authentication techniques many cryptographic algorithms were used. Those techniques used text cryptography, but in our implementation we are using image as password. For this, we will share an image with the user and server by splitting them using KNN and Huffman Algorithm.

(A) KNN Sharing-

Visual cryptography is a special type of encryption technique where visual information (Image, Text etc.) gets encrypted in such a way that decryption can be performed by Human Visual System with a computation free decryption process. The beauty of the visual secret sharing scheme is in its decryption process where without any complex cryptographic computation encrypted data is decrypted using Human Visual System (HVS). But the encryption technique needs cryptographic computation to divide the image into a number of parts let n such that at least a group of k shares out of n shares reveals the secret information, less of it will reveal no information. In this paper we have discussed a technique called random sequence which needs very less computation for k-n secret sharing.

(B) OTHER PROPOSABLE ALGORITHM FOR SECURE AUTHENTICATION-

(i)K-means Algorithm-

Basically K-Means runs on distance calculations, which again uses "Euclidean Distance" for this purpose. Euclidean distance calculates the distance between two given points using the following formula:

DOI10.17148/IJARCCE.2017.63218

Euclidean Distance = $\sqrt{(X_1 - X_2)^2 + (Y_1 - Y_2)^2}$

Above formula captures the distance in 2-Dimensional space but the same is applicable in multi-dimensional space as well with increase in number of terms getting added. “K” in K-Means represents the number of clusters in which we want our data to divide into. The basic restriction for K-Means algorithm is that your data should be continuous in nature.

(ii)Edge Detection-

Since edge detection is in the forefront of image processing for object detection, it is crucial to have a good understanding of edge detection algorithms. Edges in images are areas with strong intensity contrasts. Edge detection refers to the process of identifying and locating sharp discontinuities in an image. The discontinuities are abrupt changes in pixel intensity which characterize boundaries of objects in a scene. Classical methods of edge detection involve convolving the image with an operator. There is an extremely large number of edge detection operators available, each designed to be sensitive to certain types of edges.

Fig. 1. Example of Image password of dimension 50*50 used during login Authentication Process

Fig.2. Example of first half of the 50*50 used image password during login Authentication process stored on server side.

Fig. 3. Example of second half of the 50*50 used image password during login Authentication process sent to user email portal.

2. SECURE FILE SHARING IN WEB PORTALS-

AES and DCT Algorithm-

AES Algorithm, AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm.AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.128-bit encryption is a data/file encryption technique that uses a 128-bit key to encrypt and decrypt data or files. It is one of the most secure encryption methods used in most modern encryption algorithms and technologies. 128-bit encryption is considered to be logically unbreakable.

How safe is AES 256 bit encryption?

AES-256 is used among other places in SSL/TLS across the Internet. It's considered among the top encryptions. In theory it's not crack able since the combinations of keys are massive. Although NSA has categorized this in Suite B, they have also recommended using higher than 128-bit keys for **encryption**.

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

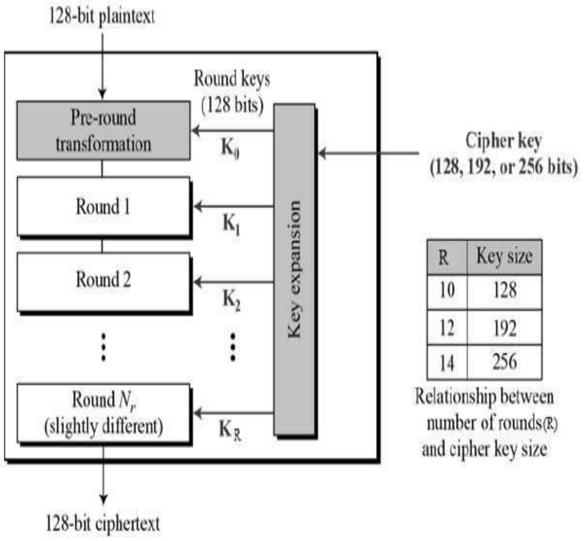

Fig. 4. AES process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 3, March 2017

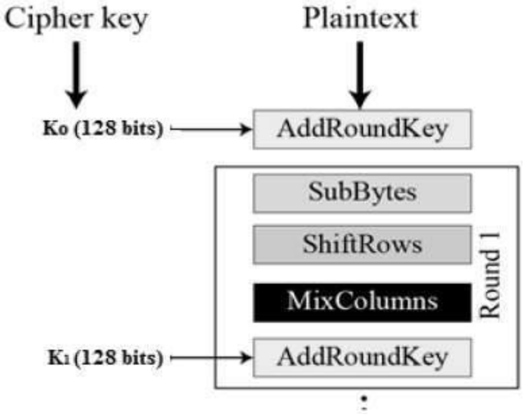

Fig. 5. Cipher Key mechanism in AES

DCT Algorithm for WaterMarking-
The discrete cosine transform (DCT) is a technique for converting a signal into elementary frequency components. It is widely used in image compression. The Discrete Cosine Transform (DCT) is a technique that converts a spatial domain waveform into its constituent frequency components as represented by a set of coefficients. The process of reconstructing a set of spatial domain samples is called the Inverse Discrete Cosine Transform (IDCT). There were two types of digital watermarking, which were the time-domain watermarking and the frequency-domain watermarking. The time-domain watermarking means that the original content would combine with the watermark information on the time-domain. It can be shown by the formula:

$$f(t)=x(t)+a(t)$$

3. Implementation Flow Diagram-

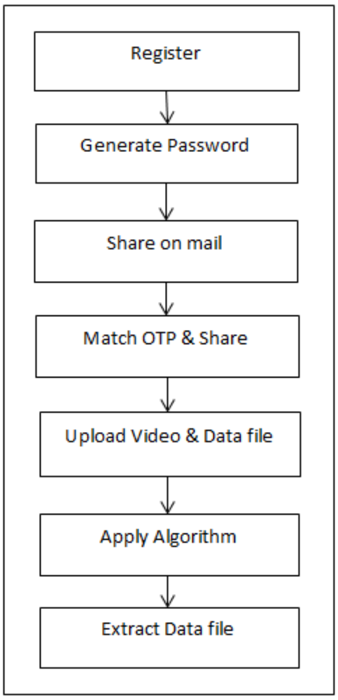

Fig. 6 Flow Diagram

II. CONCLUSION

This system we discussed in the introduction deals with different types of Visual Cryptography schemes.
Compares the image quality and security using various visual cryptography schemes. We provide the image based authentication, Password image is generated and it will be downloaded from the email which is stored at the time of registration.
The data file will be embedded using image as key into the video file and sender sends this file to the receiver and the receiver extracts the data file by using the image as a key.

REFERENCES

1. M. Naor and A. Shamir, “Visual cryptography,” in Proc. Eurocrypt’94LNCS 950. 1995, pp. 1–12.
2. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Visual cryptography for general access structures, Inform. Computation, Vol. 129, No. 2 (1996) pp. 86–106.
3. M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural images,” in Proc. WSCG Conf. 2002, 2002, pp. 303–412.
4. Stefan Droste, “New results on visual cryptography,”CRYPTO ’96 Springer-Verlag LNCS, vol. 1109, pp. 401-415, 1996.
5. M Zeghid, M Machhout, L Khriji, A Baganne,”A modified AES algorithm for image encryption,” in International journal of computer science,2007.
6. A Al-Haj, “Combined DWT and DCT digital image watermarking,” in Journal of Computer Science, 2007.
7. H Zhang, AC Berg, M Maire, “K nearest neighbour classification for visual category recognition,” in Computer vision and pattern recognition,2006 IEEE computer society conference.

BIOGRAPHIES

Pankaj Sonune is currently pursuing his Bachelors in Computer Engineering from Smt.Kashibai Navale College Of Engineering. His area of interest is Image processing.

Shikhar Srivastava is currently pursuing his Bachelors in Computer Engineering from Smt. Kashibai Navale College Of Engineering. His area of interest is Image processing.

Tushar Sonawane is currently pursuing his Bachelors in Computer Engineering from Smt. Kashibai Navale College Of Engineering. His area of interest is Artificial Intelligence.

Sourav Sengupta is currently pursuing his Bachelors in Computer Engineering from Smt. Kashibai Navale College Of Engineering. His area of interest is Artificial Intelligence dealing with pattern recognition.

DOI10.17148/IJARCCE.2017.63218