VISUAL CRYPTOGRAPHY USING COLOR PALETTE

R. Mangai Begum, M.Geevathi, G.Rajeswari
[1]Assistant Professor, [2]Student, [3]Student
[1]Department Of Informtion Technology,
[1]St.Joseph's College(Autonomous), Trichy-620 002, India.

Abstract : Visual cryptography is a method for protecting image-based secrets that has a computation-free decoding process. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc...) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers. As network technology has been greatly advanced, much information is transmitted via the Internet conveniently and rapidly. At the same time, the security issue is a crucial problem in the Palettes. In this paper proposed a visual cryptographic system using Color Palettes. In this Encryption and Decryption you can easily encrypt and decrypt text (message), so you can send emails from home or office in a safe way. The proposed method is a simple, practical and effective cryptographic system. The text information is encrypted and stored in the color Palette image. Initially user has to give the secret key in order to encrypt the text. Later, when the recipient decrypts the text, the secret key user enters is and compared with the stored color palette image. And, in case, if the secret key matches the recipient entered stored key, encrypted message will be successfully decrypted. If the recipient enters wrong key, User will get an error message "Wrong Secret Key".

IndexTerms - Visual cryptography; Decrypt; Encrypt

I. INTRODUCTION

Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images[7]. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Existing proposed the basic model of visual cryptography, researchers have published many related studies. Most of these studies, however, concentrate on binary images; few of them proposed methods for processing gray-level and color images. Proposed three methods for visual cryptography of gray-level and color images based on past studies in black-and-white visual cryptography, the halftone technology, and the color decomposition method. Our methods using of AES algorithm[6] not only retain the advantages of black-and-white visual cryptography, which exploits the human visual system to decrypt secret images without computation, but also have the backward compatibility with the previous results in black-and-white visual cryptography, such as the *t* out of *n* threshold scheme, and can be applied to gray-level and color images easily.

II. BACKGROUNDWORK:

THE EXISTING SYSTEM FOR THIS PROJECT THE TEXT INFORMATION IS ENCRYPTED BY ASCII[10] VALUES, OR ANY SPECIAL CHARACTERS. IN THE EXISTING SYSTEM, DIDN'T USE THE SAFELY SENT THE ENCRYPTED INFORMATION INTO THE MAIL. THE HACKERS EASILY ACCESS THAT INFORMATION. THE ENCRYPTED TEXT IS DIDN'T RESTRICT ANY SECRET KEY. SO THAT INFORMATION EASILY DECRYPTED.PROPOSED FOR THIS PAPER, THE TEXT INFORMATION IS ENCRYPTED BY COLOR PALETTE IMAGES. EACH USER HAS CREATED INDIVIDUAL ACCOUNT, AND THEN THEY ACCESS THEIR REQUIRED PAGES. THE USER'S PASSWORD IS CONVERTING INTO ASCII FORMAT AND STORED INTO THE DATABASE. SO ANY HACKERS OR ADMIN ALSO SHOULD NOT FIND OUT THE PARTICULAR USER'S PASSWORD DETAILS. THE USER'S INFORMATION IS PROTECTED INTO SPECIFIC SECRET KEY ENTERED BY USER. THE SECRET KEY IS CONVERTING INTO ASCII FORMAT AND STORED TO DATABASE. WHENEVER THE USER HAS DECRYPTED THEIR ENCRYPTED INFORMATION, THEY SHOULD ENTER THE CORRECT SECRET KEY. AND USER SENDS ANY SECURE INFORMATION, IT WAS ENCRYPTED AND ITS LINK ONLY SENT TO THE MAIL.

III. COMPONENTS OF VISUAL CRYPTOGRAPHY USING COLOR PALETTE

3.1 Create Color Palette Image

Small color images are created by PHP GD functions. Each text has assigned to particular images. The color palette images and its relevant information are stored into the database.

3.2 Encrypt the text

The user has to register their name and their details. The registered information will be stored in the database. User or administrator tries to check this site and entered correct login username and password. After that, this application checks to redirects the required pages for administrator as well as user. The user has entered their important information, each text has convert to particular images. The images are randomly allocated to each text. Then image names only stored to database.

3.3 Send the encrypted text to Mail with web links

The user enter the information, and then send to particular mail address. User's information is stored into the database for encrypted[7] format. So web link with information's ID only sent to the mail. The mail has sent by SMTP[11] protocol. This process only worked on any online domain. Otherwise we will try to install the SMTP protocol.

3.4 Retrieve the web links from mail

Receiver is click this link, then open into this website. The receivers enter the secret key, if it is check with database, after they will retrieve the decrypted information.

3.5 Decrypt the Text

The user's secret information are stored into the database, these information displayed only color palette format. After the user is enter the secret key, if there are compare with database, and the information is decrypted. Then the user is view their information.

4. DESIGN METHODOLOGY

4.1 AES ALOGRITHM

In January, 1997 NIST began its effort to develop the AES[6], a symmetric key encryption algorithm, and made a worldwide public call for the algorithm to succeed DES. Initially 15algorithms were selected, which was then reduced down to 4 algorithms, RC6, Rijndael, Serpent and Two-fish, all of which were iterated block ciphers. The four finalists were all determined to be qualified as the AES. The algorithm had to be suitable across a wide range of hardware and software systems. The algorithm had to be relatively simple as well. After extensive review the Rijndael algorithm was chosen to be the AES algorithm.

Contents	DES	AES
Date	1976	1999
Block Size	64	128
Key Length	56	128,192,256
Number Of Rounds	16	9,11,13
Encryption Primitives	Substitution, Permutation	Substitution, Shift, Bit Mixing
Cryptographic Primitives	Confusion ,Diffusion	Confusion ,Diffusion
Design	Open	Open
Design Rationale	Closed	Open
Selection Process	Secret	Secret, But Accept Open Public Comment
Source	IBM, Enhanced By NSA	Independent Cryptographers

Figure 4.1 Difference between DES and AES

4.2 THE ALGORITHM IS BASED ON AES KEY EXPANSION TECHNIQUE

AES Key Expansion technique in detail.

4.1 AES Key Expansion

Pseudo code for AES Key Expansion: The key-expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x (Nr+1) words. Where Nr is the number of rounds.

The process is as follows,

- The first four words are made from the cipher key (initial key). The key is considered as an array of 16 bytes (k0 to k15). The first four bytes (k0 to k3) become w0, the four bytes (k4 to k7) become w1, and so on.
- The rest of the words (wi for i=4 to 43) are made as follows

i) If (i mod 4) != 0, wi=wi-1 xor wi-4.

ii) If (i mod 4) = 0, wi=t xor wi-4. Here t is a temporary word result of applying SubByte transformation and rotate word on wi-1 and XORing the result with a round constant.

4.2 Modifications in AES Key Expansion

Certain changes made in the above key expansion[5] process improves the encryption quality, and also increases the avalanche effect. The changes are

a) The Rcon value is not constant instead it is being formed from the initial key itself, this improves the avalanche effect.

b) Both the s-box and Inverse s-box are used for the Key Expansion[5] process which improves nonlinearity in the expanded key and also improves the encryption quality.

c) We do not use the S-box and Inverse S-box as such for this algorithm; instead we perform some circular shift on the boxes based on the initial key this improves the key sensitivity.

4.3 Steps Involved

a) Key Selection

The sender and receiver agree upon a 128 bit key. This key is used for encryption and decryption of images. It is a symmetric key encryption technique, so they must share this key in a secure manner. The key is represented as blocks k[0],k[1]...k[15]. Where each block is 8bits long (8*16=128 bits).

b) Generation of Multiple keys

The sender and receiver can now independently generate the keys required for the process using the above explained Modified AES Key Expansion technique. This is a one time process; these expanded keys can be used for future communications any number of times till they change their initial key value.

c) Encryption

Encryption is done in spans, where we process 16 pixels in each span. For both its Cipher and Inverse Cipher, the AES algorithm[9] uses a round function that is composed of four different byte oriented transformations: SubBytes, ShiftRows, MixColumns and AddRoundKey.

d) Decryption

The decryption process is similar as encryption, but we use Inverse SubByte Transformation.

The whole AES structure is

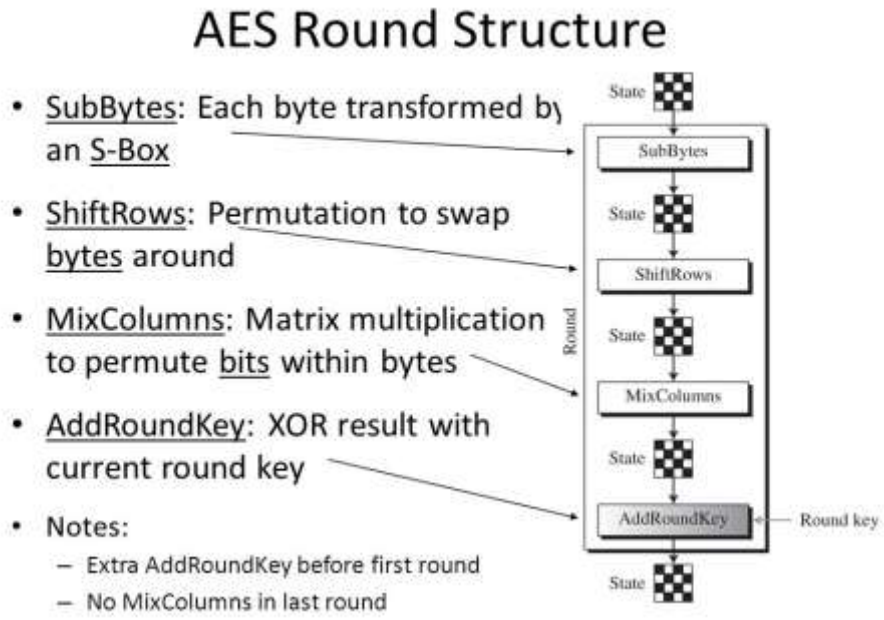

Figure 4.3 AES Structure

FUTURE ENHANCEMENT AND CONCLUSION

This paper "VISUAL CRYPTOGRAPHY" is developed successfully and it is very useful for the text information is encrypted and stored in the Color Palette image. Each user has created individual account for this website, and then they are adding their important information encrypted by color palettes. Whenever the user has needed that information, they enter the secret key, after that decrypt their information. And user has sent the encrypted information's link to mail. Then click the link and decrypt their information. This paper will help users to send and receive the information securely and those image encrypt and decrypt by using of AES Algorithm while offers a encryption quality. Time required of AES Algorithm[6] is less than DES Algorithm and future development of this project is to provide more security to chatting data using cryptography technique. Due to these features the algorithm makes of avoid the difficulties present in real time application.

References

[1]Kevin Tatroe, Rasmus Lerdorf, Peter Mac Intyre, "Programming php", 3rd Edition,O'Reilly Media,March 2002.

[2] Vikram Vaswani, "mysql: The Complete Reference", 1st Edition, McGraw Hill Osborne Media, 18th December 2003.

[3] Roger S.Pressman "Software Engineering: A Practitioner's Approach" ,7th Edition,28th January 2016.

[4] C.J.Date,A.Kannan and S.Swamynathan, "An Introduction To Database System", Pearson Education,8th Edition,2009.

[5] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu, Image Encryption Based on AES Key Expansion, 2011 Second International Conference on Emerging Applications of Information Technology 978-0-7695-4329-1/11.

[6] About AES – Advanced Encryption Standard, Copyright 2007 Svante Seleborg Axantum Software AB.

[7] P.karthigaikumar, Soumiya Rasheed, Simulation of Image Encryption using AES Algorithm , IJCA Special Issue on Computational Science - New Dimensions & Perspectives NCCSE, 2011, 166-172.

[8] Irfan AbdulGani Landge, Implementation of AES Encryption and Decryption using VHDL, International J. of Engg. Research & Indu. Appls. (IJERIA). ISSN 0974-1518, Vol. 4, No. III (August 2011), 395-406.

[9] Priyanka Chauhan and Girish Chandra Thakur, "Efficient Way of Image Encryption UsingGeneralized Weighted Fractional Fourier Transform with Double Random Phase Encoding" International Journal of Advanced Research in Engineering & Technology (IJARET), Volume 5, Issue 6, 2014, pp: 45 – 52.

[10] Shirley,R (August 2007),Internet Security Glossary,Version 2,RFC 4949,archieved from the original on 2016.

[11] SMTP (simple mail transfer protocol), Vladimir V.Riabov published by 29 NOV 2011, https://doi.org/10.1002/9781118256114 ch26.