Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Privacy Enhanced Online Payment System

Malathy.S[1], Sharmila .B[2], Sushmitha .L[3]
[1]Assistant professor,Department of Information Technology
[2,3]UG Scholar, Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, India

Abstract-A new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft has been proposed. When you make a payment, the information will never be passed on your personal financial details to merchant sites, keeping your data safe and your identity protected against fraud. A cryptographic technique based on visual secret sharing is 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 un-trusted communication channel. Only combining the k shares or more give the original secret image. Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc., from unsuspecting victims for identity theft, financial gain and other fraudulent activities The use of images is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Several solutions have been proposed to tackle phishing.

Keywords-Steganography; Visual Cryptography, Phishing; Information Security

I. INTRODUCTION

A payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. If the user forget the secure ID and account ID, it can be easily retrieved with the protection. So, automatically privacy is enhanced here. The method is concerned only with prevention of identity theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography methods are basically applied for physical banking, the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier. Today, the online project is becoming more popular. Identity theft and phishing are the common dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information for making purchase and opening of bank accounts or arranging credit cards. In 2012 consumer information was misused for an average of 48 days as a result of identity theft. Phishing is also a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. In 2nd quarter of 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others.

II. ABOUT STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Cryptography involves converting a message text into an unreadable cipher. On the other hand, steganography embeds message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks. Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion. In this paper we propose an advanced system of encrypting data that combines the features of cryptography, steganography along with multimedia data hiding. It also includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. This system will be more secure than any other these techniques alone and also as compared to steganography and cryptography combined systems

Steganography is the art of "secret communication". Its goal is to transmit a message (information) hidden inside another visible message. The typical visible message used in many steganography systems is a digital image and the embedded message is usually hidden by working in the Fourier domain. The message is first coded by a sequence of small irregular images and then merged inside another image together with many other small images.The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—will arouse interest, and may in themselves be incriminating in countries where encryption is illegal.

Visual steganography is one of the most secure forms of steganography available today. It is most commonly implemented in image files. However embedding data into image changes its colour frequencies in a predictable way. To overcome this predictability, we propose the concept of multiple cryptography where the data will be encrypted into a cipher and the cipher will be hidden into a multimedia image file in encrypted format. We shall use traditional cryptographic techniques to achieve data encryption and visual steganography algorithms will be used to hide the encrypted data.

III.RELATED WORK

A. Basic Overview on Cryptography

Cryptography involves converting a message text into an unreadable cipher. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers The two types of algorithms that will be discussed are

- Joint Key Cryptography (Symmetric Key Cryptography): Uses a single key for both encryption and decryption
- Public Key Cryptography (Asymmetric Key Cryptography): Uses one key for encryption and another for decryption

1. The joint key Cryptography: (Symmetric key cipher)

It uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message. Joint key cipher algorithms are less complex and execute faster as compared to other forms of cryptography but have an additional need to securely share the key. In this type of cryptography the security of data is equal to the security of the key.A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. The difficulty of securely establishing a secret key between two communicating parties, when a secure channel does not already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world. In other words it serves the purpose of hiding a smaller key instead of the huge chunk of message data.

2. The Public Key Cryptography (asymmetric key cipher)

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption. It is a technique that uses a different key for encryption as the one used for decryption. Public key systems require each user to have two keys – a public key and a private key (secret key). The sender of the data encrypts the message using the receiver’s public key. The receiver then decrypts this message using his private key. This technique eliminates the need to privately share a key as in case of symmetric key cipher. Asymmetric cryptography is comparatively slower but more secure than symmetric cryptography technique. The public key cryptography is a fundamental and most widely used technique, and is the approach which underlies Internet standards such as Transport Layer Security (TLS). The most common algorithm used for secret key systems is the Data Encryption Algorithm (DEA) defined by the Data Encryption Standard (DES)

3. A Hybrid Cryptosystem

A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. *It* can be constructed by using any two separate cryptosystems. It is a more complex cryptography system that combines the features of both joint and public key cryptography techniques. We shall use traditional public key cryptography techniques to covert the message into a cipher. For embedding the cipher into images, a modified joint key technique will be used.

B. Basic overview on steganography

Steganography is the art of hiding the existence of the communication message before sending it to the receiver. It has been practiced since 440 B.C. in many ways like writing information on the back of cattle in a herd, invisible ink etc. Some relatively modern ways include hiding the information in newspaper articles and magazines etc.

The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another". Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements

•The cover media(C) that will hold the hidden data
•The secret message (M), may be plain text, cipher text or any type of data
•The stego function (Fe) and its inverse (Fe-1)
•An optional stego-key (K) or password may be used to hide and unhide the message. The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media (S). The schematic of steganographic operation is shown below.

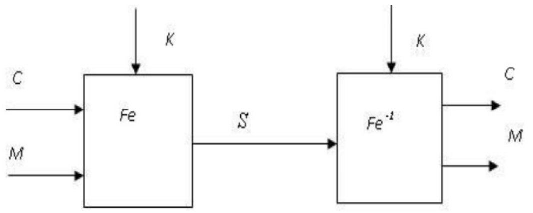

Fig.1 The Steganographic operation

Multimedia steganography is one of the most recent and secure forms of steganography. It started in 1985 with the advent of the personal computer applied to classical steganography problems. Visual steganography is the most widely practiced form of steganography and is usually done using image files. It started with concealing messages within the lowest bits of noisy images or sound files. Images in various formats like jpeg have wide colour spectrum and hence do not reflect much distortion on embedding data into them.

We shall perform steganography on image files and we shall hide the encrypted message into image files in an encrypted format thus achieving a multiple cryptographic system. The most commonly used technique for image steganography is bit insertion where the LSB of a pixel can be modified. The fourth point explains various other techniques involve spread spectrum, patch work, JPEG compression etc. Instead of traditional LSB encoding, we will use a modified bit encoding technique to achieve image steganography in which each pixel will store one byte of data.

C. Multimedia image files

Multimedia content basically comprises of images, videos and audio files. Images form the basis of visual multimedia. Multimedia is usually recorded and played, displayed, or accessed by information content processing devices, such as computerized and electronic devices, but can also be part of a live performance. Multimedia devices are electronic media devices used to store and experience multimedia content. Videos are streams of images displayed in sequence at a certain speed. We shall focus on image files to achieve visual steganography.

Images are visual data stored in a picture frame. Images basically are made up of various regions consisting of pixels. These pixels in turn consist of three basic colours R (red), G (green) and B (blue). The pixel values (R, G, B values) can be manipulated to hide data in the images. A marginal deviation in these pixel values does not alter the images as a whole but a slight shade difference occurs in the altered region that is not visible in normal conditions. The image can hence serve as a cover for the information so as to achieve steganography. The edited image can be transmitted to the receiver along with the original image. The receiver then can decode the data from the image by pixel based image comparison. The process involved in encoding and decoding uses a blend of media cryptography and asymmetric cryptographic algorithms.

An image or a multimedia data has 5 + 1 properties which include the position of colour pixel on the x-axis, the position of colour pixel in the y-axis, the R component of colour, the G component of colour, the B component of colour and the sixth is the image description properties like size, timestamp etc. These properties are stored in the first few lines of image property description. The number of bits per pixel is also a property that varies in different images. To achieve a more general bit encoding system we shall use 8-bits per pixel image.

D. Visual Cryptography

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Either transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

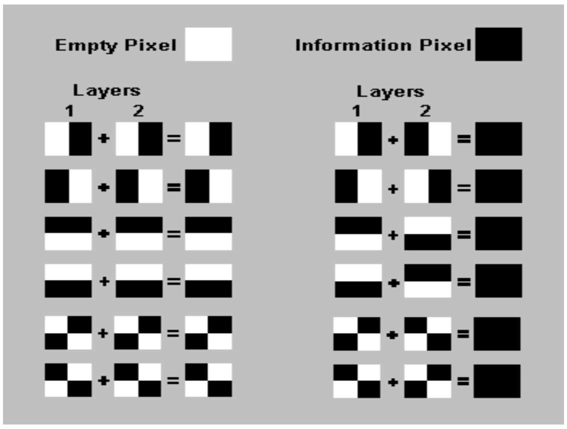

Fig.2.Representation of Pixels in Visual Cryptography

When the random image contains truly random pixels it can be seen as a one time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc). You can also copy and past them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.

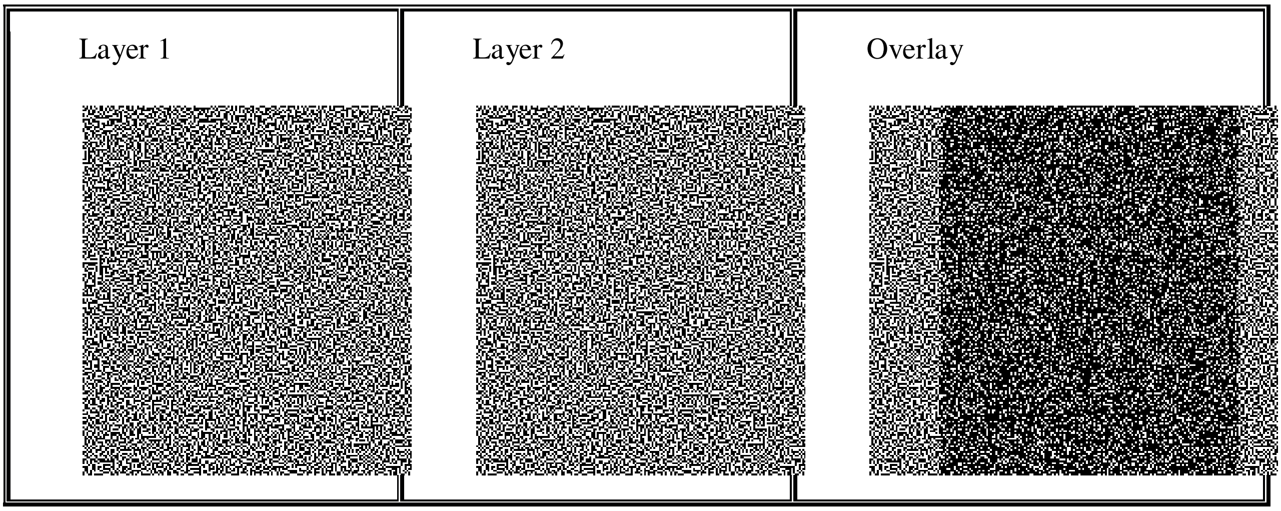

Fig. 3 Layers in Visual Cryptography

1. How Visual Cryptography works

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.

In the table on the right we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gray, and the areas with opposite states will be black. If both layers are just opposite or diagonal, the original images will be displyed in the black colour.

The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with colour pixels.

If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

IV. EXISTING SYSTEM

- The existing system supports with only one type of image format only. For example, if it is .jpg, then it supports only that same kind of image format only.
- The existing system does not provide a friendly environment to encrypt or decrypt the data (images).
- The existing visual cryptography schemes that are used for data hiding have a security hole in the encrypted Share file.
- Here an image based authentication using Visual Cryptography is implemented.

Algorithm:

Text based steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a sentence. This gives flexibility and freedom from the point view of sentence construction but it increases computational complexity. The steganography technique is based on Vedic Numeric Code in which coding is based on tongue position. For applying the Vedic code to English alphabet, frequency of letters in English vocabulary is used as the basis for assigning numbers to the letters in English alphabet. Number assignments of letters are shown in table 1. No separate importance is given for vowels and consonants as compared.

Each letter is assigned a number in the range of 0 to 15. For different frequencies, different numbers are assigned to the letters. Number assigned in range (N+0.99) % to (N+0.3) % and (N+0.2) % to (N+0.01) % is same where N is any integer from 0 to 11. It basically represents frequency of letters in integer form. Above number assignment method is used to maximize no of letters in a particular assigned number group which in turn gives flexibility in word choosing and ultimately results in suitable sentence construction.

A. Encoding

Steps:

- Representation of each letter in secret message by its equivalent ASCII code.
- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts.
- Choosing of suitable letters from table 1 corresponding to the 4 bit parts.
- Meaningful sentence construction by using letters obtained as the first letters of suitable words.
- Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.
- Encoding is not case sensitive.

B. Decoding

Steps:

- First letter in each word of cover message is taken and represented by corresponding 4 bit number.
- 4 bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

C. Drawback

In result to hide 4 letter word, 8 words are required excluding the words that are added to provide flexibility in sentence construction. So to hide a large message, this technique requires large no of words and creates a complexity in sentence construction. Disadvantage of this technique can be used in its advantage by applying it to online banking to create spam mail to hide one's banking information.

- Does not provide a friendly environment to encrypt or decrypt the data (images).
- Supports with only one type of image format only. For example, if it is .jpg, then it supports only that same kind of image format only.
- The most critical measurements to evaluate the effectiveness of a VCS.

V. PROPOSED SYSTEM

- Proposed System Visual Cryptography (VC), technique based on visual secret sharing used for image encryption.
- Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant.
- In this paper, a new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant.
- VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system.
- For phishing detection and prevention, we are proposing a new methodology to detect the phishing website.
- Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.
- Cryptographic technique :(2, 2) - Threshold VCS scheme, (n, n) -Threshold VCS scheme, (k, n) Threshold VCS scheme are used in this proposed system.
- Cryptographic algorithms generally need a reference table which aids the conversion of a small block of data into another block (may not be a block of data in the original content).
- In order to provide higher security levels the algorithm is designed to use a reference database as shown in Fig. 2. The reference database will consist of various reference grids. Each of

these grids will have a 3-d representation of the encoding schema which will be used to represent the characters in terms of specific numbers. (The same number may or may not represent a different character in a different grid).

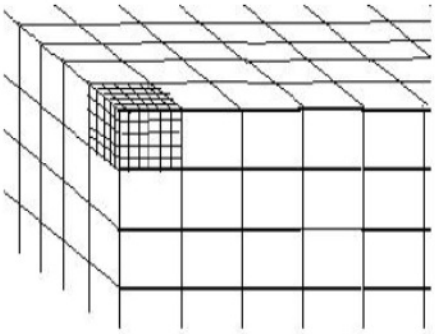

Fig. 4 Matrices in a Grid of the Reference database

A .Encryption Algorithm

- The message will first be encrypted using Asymmetric Key Cryptography technique. The data will be encrypted using basic DES algorithm. This cipher will now be hidden into a multimedia file.
- The cipher will be saved in the image using a modified bit encoding technique by truncating the pixel values to the nearest zero digit (or a predefined digit) and then a specific number which defines the 3-D representation of the character in the cipher code sequence can be added to this number. For every character in the message a specific change will be made in the RGB values of a pixel. (This change should be less than 5 for each of R,G and B values) This deviation from the original value will be unique for each character of the message. This deviation also depends on the specific data block (grid) selected from the reference database. For each byte in the data one pixel will be edited. Thus one byte of data will be stored per pixel in the image.
- In this method the cipher sequence can be decoded without the original image and only the edited image will be transmitted to the receiver.
- In the first few lines of image properties, the attributes of the image will be encrypted and saved so as to provide us the information if the image is edited or modified or the image extension has been changed like jpg to gif. These properties can be used in the decoding (identifying the correct block of data from the data grid). So only the correct encrypted image in the correct format will produce the sent message.
- For decryption, the receiver must know which image to decode and in which format as changing the image format changes the colour distribution of the image. Every image gives a random data on decryption that has no meaning. But only the correct Format decryption gives the original message.
- After hiding the data in the image, the image will be sent to the receiver. The receiver should have the decryption key (private key) which will be used to decode the data.

B. Decryption Algorithm

- The message can be decoded using an inverse function (as used in traditional techniques) using the receiver's private key. This key can be a part of the image or a text or any attribute of the image.
- The receiver's private key is used to identify the reference grid from the reference database.
- After selecting the correct grid, the x and y component of the image can define the block that has been used to encrypt the message and the RGB values can point to the data in the block identified by the x, y component as shown in Fig. 5.

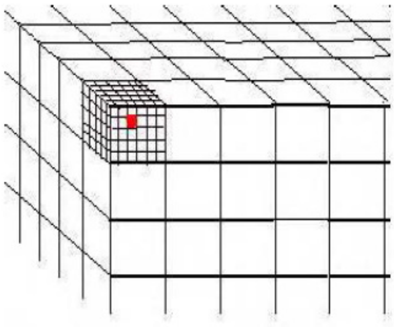

Fig.5 Identification of the correct grid in a Reference Database

- The cipher is retrieved by obtaining the difference in the pixel value from the closest predefined value (zero truncation). These numbers will now define the saved bit and will form the cipher text.
- This cipher can now be decrypted using an inverse function of the DEA algorithm to get the message text.

C. Advantages:

- Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography.
- It prevents password and other confidential information from the phishing websites.
- For phishing detection and prevention, we are proposing a new methodology to detect the phishing website.

VI. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, a payment system for online shopping is proposed with the aim to simplify the complex and redundant process with the flexibility of a simple process. It is being developed as an attempt to overcome the difficulties of the existing system. It provides two levels of security to the information being transmitted. That is the intruders cannot easily break the system as they cannot easily recognize the data, since data is hidden in two ways. This system overcomes the demerits of using single level of hiding. That is either using cryptography or steganography. And one more thing to add is it requires only the computation time of single level hiding, because visual cryptography requires no computation to decrypt the information. This method can be used to increase the security on web based applications. The user will be asked to provide the secret key and the password can be compared from image files using the key. It can be used as advancement over the existing option to input the security phrase in various web based applications. In the case of a secret message being transferred the information can be kept inside a multimedia data which will be the normal cipher which had to be transferred. This multimedia data can be transferred in the normal way. Video files and image streams can also be used to transmit data. In case of image streams part of message can be sent in each image. This will increase the security of the system, however the time consumption will increase in this case.

REFERENCES

[1] Jihui Chen,Xiayao Xie, and Fengxuan Jing, “The security of shopping online,” Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp 4693-4696, 2011.

[2] Walter Bender, Daniel Gruhl , Norshige Morimonto, A.Lu, “Techniques for data hiding,” IBM Systems Journal, Vol. 35, Nos 3&4, pp.313-336 , 1996.

[3] Javelin Strategy & Research, “2013 Identify Fraud Report,” https://www.javelinstrategy.com/brochure/276.

[4] J.C.Judge, “Steganography: Past, Present, Future,” SANS Institute, November 30, 2001.

[5] Daniel Gruhl, Anthony Lu, Walter Bender, “Echo Hiding,” Proceedings of the First International Workshop on Inormation Hiding, pp 313-336, 1996.

[6] K.Bennet, “Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding information in Text,” Purdue University, Cerias Tech Report 2004-2013.

[7] M. Naor and A.Shamir, “Visual Cryptography,” Advances in Cryptography: EUROCRYPT’94, LNCS, vol. 950, pp.1-12,1995.

[8] Anti Phishing Working Group (APWG), “Phishing Activity Trends Report, 2013,” http://docs.apwg_trends_report_q2_2013.pdf.

[9] Bharathi Krishna Tirthaji, “Vedic Mathematics and its Spiritual Dimension”, Motilal Bansari Publishers,1992.

[10] S.Premkumar , A.E.Narayanan, “New Visual steganography scheme for Secure banking Application,” Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies(ICCEET), pp. 1013-1016, Kumaracoil, India, 2012.