An Improved Data Transfer Technique using Steganography with Water marking and Visual Cryptography

Sakshi Batra, Harpinder Kang Khattra

Abstract— Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. It is a form of security through obscurity. The word Steganography in the modern day usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. In this paper a new type of cryptographic scheme is proposed, which can decode concealed images without any cryptographic computations. The scheme is perfectly secure and very easy to implement. Further watermarking is also applied on the data so as to provide much security. Digital watermarking is the process of inserting a digital signal or pattern (indicative of the owner of the content) into digital content. The signal, known as a watermark, can be used later to identify the owner of the work, to authenticate the content, and to trace illegal copies of the work.

Index Terms— Cryptography, Steganography, Water marking, security.

I. INTRODUCTION

Information hiding techniques have been receiving much attention today. Steganography is an application of information hiding. Steganography or stego literally means "covered writing" which is derived from Greek language[1]. Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present. Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily.

Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

Visual Cryptography is a method used for encrypting a secret image into shares, such that stacking the shares reveals the secret image. Cryptography can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network. Cryptography uses two main styles or forms of encrypting data; symmetrical and asymmetrical. Symmetric encryptions, or algorithms, use the same key for encryption as they do for decryption. Other names for this type of encryption are secret-key, shared-key, and private-key. The encryption key can be loosely related to the decryption key; it does not necessarily need to be an exact copy[2].

In recent years, the distribution of works of art, including pictures, music, video and textual documents, has become easier. With the widespread and increasing use of the Internet, digital forms of these media (still images, audio, video, text) are easily accessible. This is clearly advantageous, in that it is easier to market and sell one's works of art. However, this same property threatens copyright protection. Digital documents are easy to copy and distribute, allowing for pirating. There are a number of methods for protecting ownership. One of these is known as digital watermarking. Digital watermarking is the process of inserting a digital signal or pattern (indicative of the owner of the content) into digital content. The signal, known as a watermark, can be used later to identify the owner of the work, to authenticate the content, and to trace illegal copies of the work. Watermarks of varying degrees of obtrusiveness are added to presentation media as a guarantee of authenticity, quality, ownership, and source[8].

II. SECURE COMMUNICATION

Steganography has been used in many different ways throughout time. The simplest was the use of invisible inks that a person could use to send a message to another without anyone else knowing. Different forms of invisible ink have been used to conceal messages throughout time. Some of the more common forms of invisible ink have been lemon juice, milk, and urine to name a few. If someone wanted to conceal a message they would simply write a message, using one of these inks, on a sheet of paper that already had something written on it. The person receiving the message would then hold the paper over a flame and the transparent message would appear[6].

Manuscript Received December 2013.

Sakshi Batra, M.Tech ECE Student., PTU/ Chandigarh Group of Colleges,Landran, Mohali, India.

Ast Prof. Harpinder Kang,ECE Deppt., PTU/ Chandigarh Group of Colleges,Landran, Mohali, India.

Steganography or Stego as it is often referred to in the IT community, literally means, "covered writing" which is derived from the Greek language. Steganography is defined as "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present"[3].

In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security[10].

Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. Mainly because of their popularity on the Internet and the ease of use of the steganographic tools that use these data formats[5]. These formats are also popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message.

Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Steganographic research is primarily driven by the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open-systems environment. Many governments have created laws that either limit the strength of cryptosystems or prohibit them completely. This has been done primarily for fear by law enforcement not to be able to gain intelligence by wiretaps, etc[14].

This unfortunately leaves the majority of the Internet community either with relatively weak and a lot of the times breakable encryption algorithms or none at all. Civil liberties advocates fight this with the argument that “these limitations are an assault on privacy”. This is where Steganography comes in. Steganography can be used to hide important data inside another file so that only the parties intended to get the message even knows a secret message exists. To add multiple layers of security and to help subside the "crypto versus law" problems previously mentioned, it is a good practice to use Cryptography and Steganography together. As mentioned earlier, neither Cryptography nor Steganography are considered "turnkey solutions" to open systems privacy, but using both technologies together can provide a very acceptable amount of privacy for anyone connecting to and communicating over these systems.

Sender and Receiver

Suppose a sender wants to send a message to a receiver. Moreover, this sender wants to send the message securely, She wants to make sure an eavesdropper cannot read the message.

Messages and Encryption

A message is plaintext (sometimes called cleartext). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption.

The art and science of keeping messages secure is cryptography, and it is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking ciphertext; that is, seeing through the disguise. The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology and its practitioners are cryptologists. Modern cryptologists are generally trained in theoretical mathematics—they have to be.

The concept of digital watermarking is derived from steganography. Both steganography and watermarking describe techniques that are used to keep information by embedding it into the cover data. The methods used for steganography are usually not robust against modification of the data. Digital watermarking on the other hand should be robust against attempts to remove the hidden data[15]. A popular application of watermarking is proof of ownership. As mentioned before, based on the host signal in which the watermark is embedded, watermarking may be classified as:

(a) Digital image Watermark- Both visible as well as invisible watermarking is applicable in images.

(b) Digital video Watermark- A video sequence consists of many frames that can be taken as images. Hence, the process of watermarking in images can be extended to videos also.

(c) Digital audio Watermark- Only invisible watermarking is possible.

(d) 3D Multimedia based Watermark.

Once the host signal is selected, the watermarking can be done in either the spatial domain i.e. where the watermark is directly embedded in the signal; or the frequency domain which involves applying any of the transformation techniques on the signal and then embed the watermark. Applications of digital watermarking include: copyright protection, covert communication, broadcast monitoring, content authentication, content description, and copy and usage control[12].

The purposes of Digital Watermarks

Watermarks are a way of dealing with the problems mentioned above by providing a number of services:

1. They aim to mark digital data permanently and unalterably, so that the source as well as the intended recipient of the digital work is known. Copyright owners can incorporate identifying information into their work. That is, watermarks are used in the protection of ownership. The presence of a watermark in a work suspected of having been copied can prove that it has been copied.
2. By indicating the owner of the work, they demonstrate the quality and assure the authenticity of the work.
3. With a tracking service, owners are able to find illegal copies of their work on the Internet. In addition, because each purchaser of the data has a unique watermark embedded in his/her copy, any unauthorized copies that s/he has distributed can be traced back to him/her.
4. Watermarks can be used to identify any changes that have been made to the watermarked data.
5. Some more recent techniques are able to correct the alteration as well.

The following are the various outcomes of the proposed system.

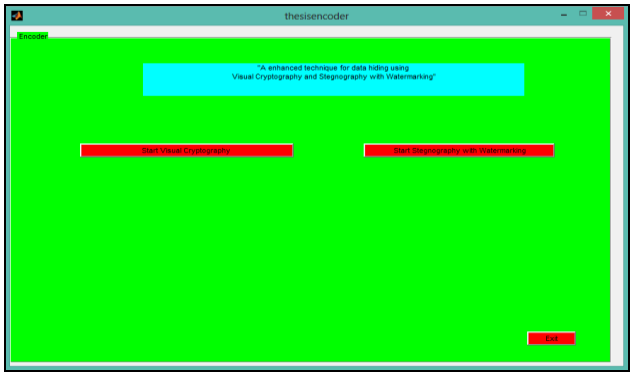

Figure1. The basic GUI of the proposed system.

On clicking on the 'start visual cryptography' button we get the following outcome. It will convert the message into shares named as share1 and share2.

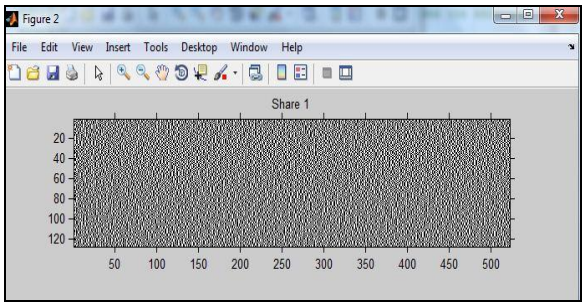

Figure 2.1 Share 1 for Cryptography

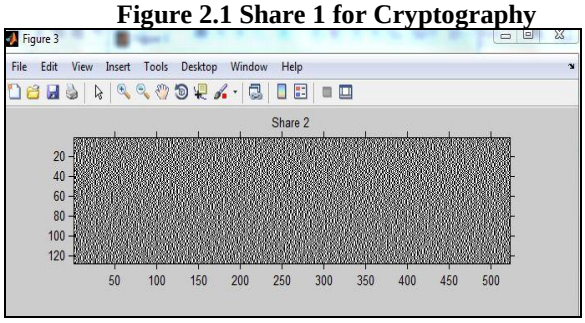

Figure 2.2 Share 2 for cryptography

The following is the outcome of the second button.

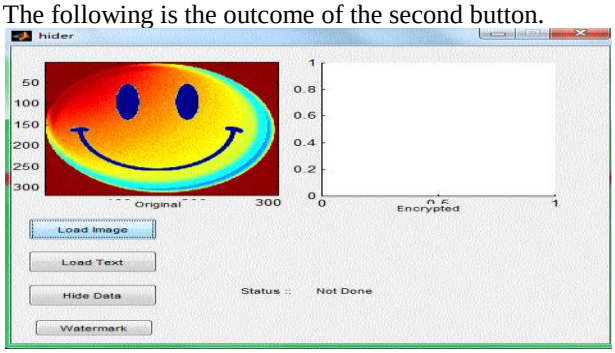

Figure3. GUI for Steganography

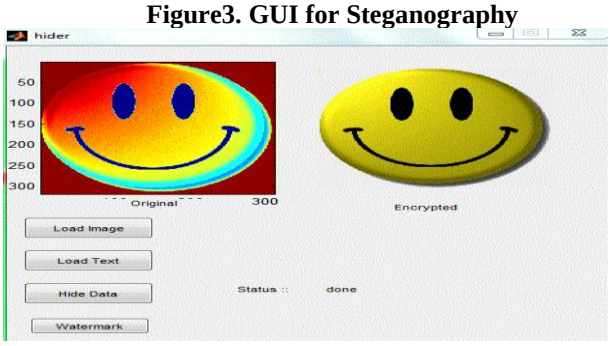

Figure4. The message is hidden and the image is encrypted.

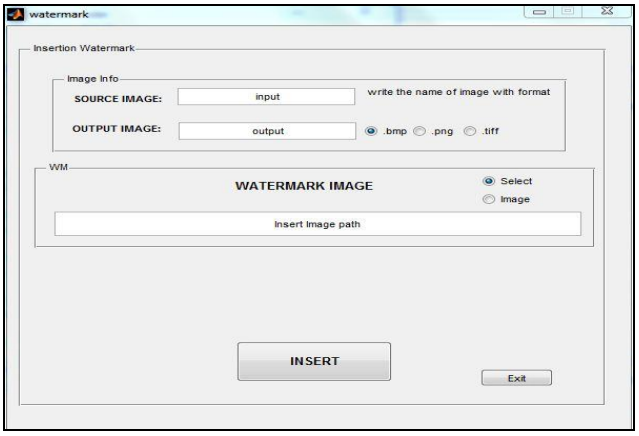

Figure5. GUI for Watermarking

The following are the outcomes on the receiver site.

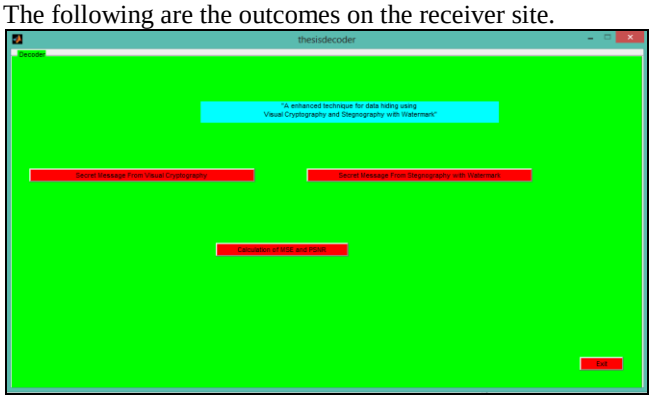

Figure 6. The layout of the GUI.

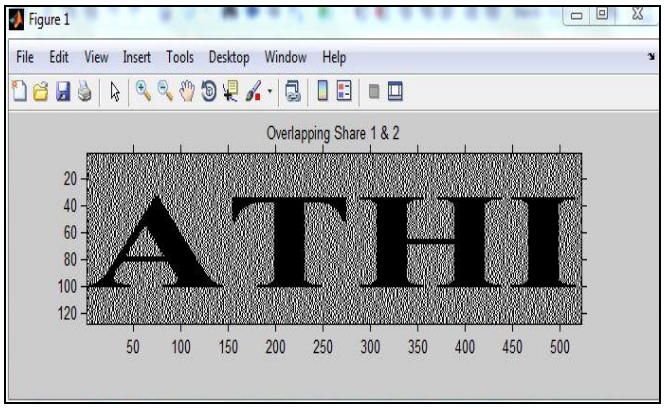

Figure 7. Data extract from Cryptography

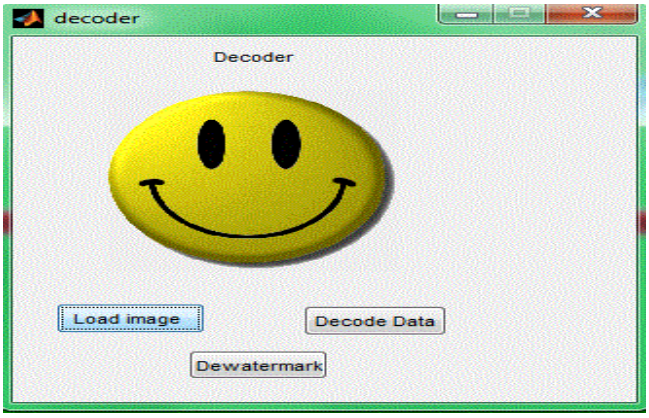

Figure8. Data extract from Steagnography.

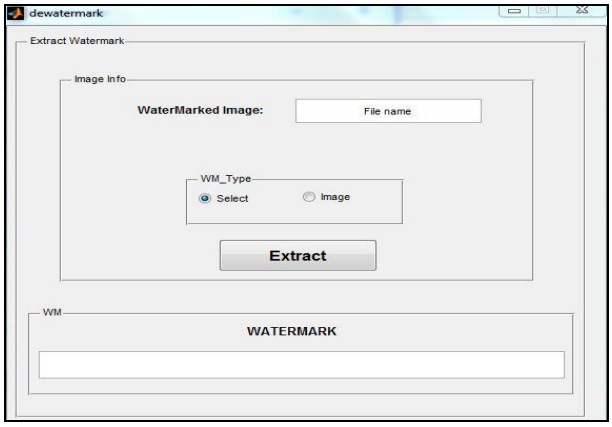

Figure9. GUI for Dewatermarking

III. CONCLUSION

The work accomplished during this paper can be summarized with the following points: In this we have presented a new system for the combination of cryptography and Steganography with Watermarking which could be proven as a highly secured method for data communication in near future. Steganography, especially combined with cryptography and watermarking is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little distortion in the image. The main advantage of this System is to provide high security for key information exchanging. This System fined applications in medicine by doctors to combine explanatory information within x-ray images. It is also useful in communications for codes self error correction. It can embed corrective audio or image data in case corruption occurs due to poor connection or transmission. The proposed High secured system using cryptography, steganography and watermarking is tested by taking message and hiding them in some images of different sizes. The results that are obtained from these experiments are recorded. Steganography is a tool to conceal high sensitive information and it is an art of hiding information in a plain sight.

REFERENCES

1. N . Provos, "Defending Against Statistical Steganography," Proc 10th USENEX Security Symposium 2005.
2. N . Provos and P. Honeyman, "Hide and Seek: An introduction to Steganography," IEEE Security & Privacy Journal 2003.
3. Steven W. Smith , The Scientist and Engineer's Guide to Digital Signal Processing.
4. Katzenbeisser and Petitcolas , "Information Hiding Techniques for Stenography and Digital watermaking" Artech House, Norwood, MA. 2000.
5. L. Reyzen And S. Russell , "More efficient provably secure Steganography" 2007.
6. S.Lyu and H. Farid , "Steganography using higher order image statistics , " IEEE Trans. Inf. Forens. Secur. 2006.
7. Venkatraman , s, Abraham , A . & Paprzycki M." Significance of Steganography on Data Security " ,Proceedings of the International Conference on Information Technology : Coding and computing , 2004.
8. Fridrich , J ., Goljan M., and Hogea , D ; New Methodology for Breaking stenographic Techniques for JPEGs. "Electronic Imaging 2003".
9. http:/ aakash.ece.ucsb.edu./data hiding/stegdemo.aspx.Ucsb data hiding online demonstration. Released on Mar .09,2005.
10. Mitsugu Iwanmoto and Hirosuke Yamamoto, "The Optimal n-out-of-n Visual Secret Sharing Scheme for GrayScale Images", IEICE Trans. Fundamentals, vol.E85- A, No.10, October 2002, pp. 2238-2247.
11. Doron Shaked, Nur Arad, Andrew Fitzhugh, Irwin Sobel, "Color Diffusion: Error Diffusion for Color Halftones", HP Laboratories Israel, May 1999.
12. Z.Zhou, G.R.Arce, and G.Di Crescenzo, "Halftone Visual Cryptography", IEEE Tans. On Image Processing,vol.15, No.8, August 2006, pp. 2441-2453.
13. M.Naor and A.Shamir, "Visual Cryptography", in Proceedings of Eurocrypt 1994, lecture notes in computer science, 1994, vol.950, pp. 1-12.
14. Swati Tiwari and R. P. Mahajan "A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion", International Journal of Electronics Communication and Computer EngineeringVolume 3, Issue 1, ISSN 2249 –071X © 2012 IJECCE,
15. E.R.Verheul and H.C.A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing scheme", Designs, Codes, and Cryptography, vol.1, no.2, 1997, pp.179-196.

AUTHORS PROFILE

Sakshi Batra is currently doing her M.Tech Degree in Electronics and Communication in Chandigarh Group of Colleges, Landran, Mohali(Punjab). She completed her B.E. degree in Electronics and Communication from Lovely Professional University, Jalandhar, India. Her area of interest includes Image Processing, Networking and Network Security.

Prof. Harpinder Kang Khattra received the B.E. degree in Electronics and Communication engineering from University College of Engineering,Punjabi University, Patiala and completed her M.E. degree in VLSI Design from Thappar University,Patiala. Currently She is working as Asst. Prof/ECE in Chandigarh Group of colleges, Landran, Mohali(Punjab). Her Area of interest includes Electronics, Photonics and Image Processing.