Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Data Hiding Using MLSB Steganography

Harleen Kour
Research Scholar
Department of Computer Science
Chandigarh University
Chandigarh, India

Surinder Kaur
Associate Professor
Department of Computer Science
Chandigarh University
Chandigarh, India

Abstract— ***Sending of data over the internet for various purposes has become a necessary part of technology now days. But, the data sent over the internet as well data to be retrieved can be hacked by any other party in several ways. To provide the secure transmission and receiving of data, various cryptographic schemes have been proposed in the last decade. Among the proposed schemes the data integrity is not ensured in a number of aspects. Hence, in this paper, Data Hiding Scheme uses Multiple Least Significant bit (MLSB) steganography, which is used to hide the data. Another scheme is also being applied in this paper named as Digital Signature Scheme Algorithm (DSA) which is used to provide security services like authentication of data. During authentication of data, the authentication key transport and authentication key agreement are provided for the data during its encryption and decryption. The simulator used for the whole process is MATLAB. The simulation results show that the applied DSA algorithm and Data Hiding MLSB schemes provide, the better hiding and data security to the data or information sent over the network.***

Keywords— ***Steganography, Cryptography, Multiple Least Significant bit (MLSB), Digital Signature Algorithm (DSA)***

I. Introduction

Cryptography is the process of doing encryption and decryption of data and to provide security or authenticity to the encrypted data over the internet. The data sent over the internet in the form of encrypted data is transformed into the cipher text from the plain text to hide the original form of data from any hacker of its misuse. Cryptography changes the form of data from one state to another which can never be understood without its proper decryption. On the other hand, Steganography is also a branch of science and technology, which transforms the encrypted data into a hidden form so that the third person can never find it [1]. Hence, Cryptography and Steganography both of the techniques are used to provide the authenticity to the data which has to be sent over the network and to hide it from its misuse. The main aim of Steganography is to keep the message undetectable from any unauthorized access. The concept of cryptography is not always as sufficient to provide the secure communication. But, the combination of both the scheme results in the secure and confidential form of data which can be kept secret easily and prevents it from any unauthorized access. The primary goal of cryptography is entirely based on the capability to hide the message from any insecurity. Essentially, the principle of cryptography and steganography is to offer secret and secure communication. Steganography can be implemented to wrap hidden messages in the form of audio, video or image and also text files [2].

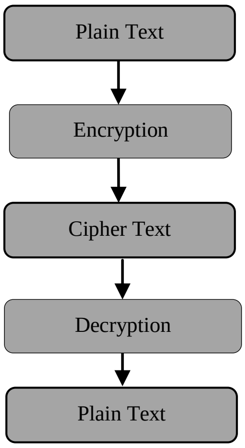


Figure 1: Encryption and Decryption in Cryptography

The above figure shows the following terms which can be described as:

- **Plain Text:** In cryptography, plain text is information a sender wishes to transmit to a receiver. Plain text has reference to the operation of algorithms using cryptographic and encryption algorithms, and is the input upon which they operate.

- **Encryption:** In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption denies the message content to the interceptor and it does not itself denies the interception.
- **Cipher Text:** It is encrypted text. Plain text is what we have before encryption, and the cipher text is the encrypted result. The term cipher is sometimes used for cipher text.
- **Decryption:** It is defined as the process of decoding data that has been encrypted into a secret form. A secret key or password is required for Decryption.

Frequently, the same cipher is used for both encryption and decryption. Thus, the difference lies in the fact that the Encryption creates a cipher text from a plain text, Decryption creates a plain text from a cipher text.

Figure 1 shows that in the process of cryptography, the plain text is encrypted first and then the decryption of encrypted text is only possible after the step of ciphering. The decryption provides the original text at the end, which is also known as plain text. The two most general techniques used for hiding data within a picture, audio and video files are LSB (Least Significant Bit) and MLSB (Multiple Least Significant Bit). In the last decade, MLSB scheme has attracted the interest of many of the researchers which are used to provide the data hiding and security to the encrypted data. The encryption algorithm used to provide the encryption and decryption of the data is of mainly two types, i.e. symmetric and asymmetric encryption [3]. The Digital Signature Scheme Algorithm (DSA) used in this paper is of asymmetric type algorithm [5].

Cryptographers have been analyzing technologies which are dealing with electronic signatures. Numerous electronic signature schemes come out to be safe and secure having some of the complexity in the theoretical hypothesis. The researchers proposed a conventional electronic signature system which is based on the server having a small number of common private keys. In this paper, the security or safety is provided for the data which is done by the application of DSA and MLSB schemes in which the data can be put into a hidden mode so that it can never be visible to any hacker for its misuse.

II. CRYPTOGRAPHY AND STEGANOGRAPHY

A. Cryptography

Cryptography is the ability of achieving security by encoding the data into an unreadable form. Cryptography is the branch of cryptology which deals with algorithm designs for encryption and decryption, leads to the genuineness of the message. A process to hide the content of encoding plain text is called encryption and to get back the cipher text to its original plain text is known as decryption. Cryptosystem proves as a unique security solution in various emerging applications concerned to electronics, communication, networks where authentication of security is necessary. It is also used to study electronic signature technologies. A server-based electronic signature system is based upon bits of transmitting messages and on a number of secret keys. In addition to this it is also used to design an off-line signature verification based on the displacement extraction method.

There are two types of encryption algorithms: symmetric encryption algorithm and asymmetric encryption algorithm [3]. In symmetric key encryption sender and receiver will have the same key for the process of encryption and decryption of data [4]. In a symmetric key encryption algorithm different keys are used in sending and receiving site for encryption and decryption. The Digital Signature Scheme Algorithm (DSA) used in this paper is of asymmetric type algorithm [5].

List of Symmetric Algorithms:

i. Data Encryption Standard (DES)
ii. Advanced Encryption Standard (AES)
iii. Blowfish Encryption Algorithm
iv. International Data Encryption Algorithm
v. Triple Data Encryption Standard

List of Asymmetric Algorithms:

i. Diffie-Hellman
ii. RSA
iii. DSA

B. Steganography

The word steganography is derived from the Greek words "*stegos"* meaning "cover" and "*grafia*" meaning "writing". The art of hidding a message, image, or file within another message, image, or file, video is known as Steganography. Steganography is used to reveal the information which is hidden in an audio or video file. To control the hiding process a stego-key is used so as to limit the detection or recovery of fixed data.

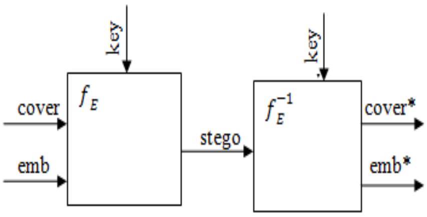


Figure 2: Steganography

Figure 2 shows the process of steganography. f_E is the stenographic function "embedding" and f_E^{-1} is the stenographic function "extracting". Cover is the coverage data in which emb will be hidden and emb is the terms related to message to be hidden. Key : parameter of f_E . Stego means the cover data with the hidden message

Steganography is a key solution with the help of which news and information can be sent without being censored and without the panic of the point being intercepted and traced back to sender. It is also possible to simply use steganography to store information on a spot. For instance, numerous sources of information like banking information, military secrets, can be stored in a cover source. When we want to unhide the secret information cover source, we can disclose our banking data and it will be impossible to prove the existence of the secret.

***Fundamental requirement for a Steganography*:**

a. **Imperceptibility:** It means that the embedded messages should not be discernible to the human eye.
b. **Embedding Capacity:** It shows the capacity of embedding the secret image.
c. **Security:** It means that the stego image should be fool proof and robust.

Thus, the logical difference between Steganography and cryptography is that cryptography focuses on keeping the contents of a message secret where as steganography focuses on keeping the existence of a message secret. Steganography and cryptography, both are the processes which are used to protect information from superfluous parties.

III. DIGITAL SIGNATURE

The Digital Signature algorithm (DSA) can be used by the recipient of a message to verify that the message has not been altered during transit as well as ascertain the creator's identity. A digital signature is an electronic version of a written signature in which the digital signature can be used in providing to the recipient or any other third party that the message was, in fact, signed by the originator itself. Digital signatures can also be generated for storing data and programs so that the integrity of the data and programs may be verified at any later time. Digital signature includes: digital signature generation and verification, DSA standard, etc. The figure 3 shows the way how a digital signature is created. The process consists of two main phases described below:

a. **Signing Process by Sender:** First a message digest (MD) is generated. A message digest is a "summary of the message that is going to be dispatched," and created by a set of hashing algorithms that were agreed by both the parties. The hashing algorithm ensures the integrity of a message by producing a completely different hash value when a single piece of the message changes. A MD combines with the sender's private key and an encrypted message digest is created, which is called the Digital Signature (DS). A digital signature is enclosed with the message and sent to the receiver.

b. **Signature Verification Process by Receiver:** Using the sender's public key, a receiver decrypts the digital signature to obtain the message digest generated by the sender. The same hashing algorithm is used by the receiver for calculating MD of receiving messages. The acquired MD value is compared with the value of sender's value. If they are identical, then the message is not altered and the originality is assured. In this phase, if by decryption of the message using the sender's public key results in a faulty message digest, then the message has been altered, and cannot be trusted. Although, it is clearly shown that the integrity of the message is maintained, but not the privacy, since the message is sent plainly. This may be suitable to a situation where confidentiality is not an issue. In order to ensure confidentiality in transmission, the message should be encrypted.

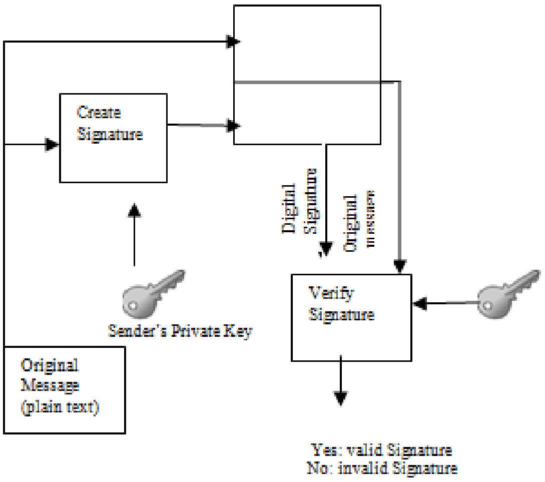


Figure 3: DSA creation

A. *Digital signature algorithm:*

DSA key generation:

1. Choose a prime q that is 160- bit long. Choose an L-bit prime p, such that p=qk+1 for some integer k, 512<=L<=1024 and L is divisible by 64.
2. Generate g:choose h, where 1<h<p-1 such that g=$h^k \bmod p$ >1 and k= (p-1)/q.

3. Secretly choose x by some random method, where 0<x<q and calculate y=$g^x\ (mod\ p)$
4. The public key is (p,q,g,y). The private key x must be kept secret. However (p,q,g,y) can be shared between different users of the system if desired.

B. DSA Signature Creation:

1. Select a random secret integer k where 0<k<q.
2. Calculate r=(g^k(mod p)) (mod p)
3. Calculate s=(k^{-1}.SHA(M)+ x.r)(mod q) where SHA(M) is the SHA-1 hash function applied to the message M.
4. The values of r and shall be checked to determine if r = 0 or s = 0. If either r = 0 or s = 0, a new value of k shall be generated, and the signature shall be recalculated. It is extremely unlikely that r =0 or s = 0if the signatures are generated properly.

Sends signature (r,s) with message M.

C. DSA signature verification:

1. Reject the signature if either 0<r<q or 0<s<q is not satisfied.
2. Calculate w = (s) mod q
3. Calculate u1 = (SHA(M)*w) mod q
4. Calculate u2 = (r*w) modq
5. Calculate v=(($g^{u1} * y^{u2}$) modp)mod q

Signature is valid if v = r.

After the DSA key generation process the signature is created. The final step of Signature creation and the first step of the signature verification insists that should not be equal to zero.

IV .Advantage Of Using Digital Signature

Various advantages of using digital signature are described:

- **Authentication:** It can help us to ensure that the data issued by the sender is not being forged by an intruder. It actually proves the identification of the person that signs.
- **Integrity:** It ensures that every change in the data is sent by the sender if any can be detected. It ensures the content of message secured and unaltered.
- **Non-repudiation:** It certifies that the sender cannot be denied of his work.
- **Confidentiality:** It ensures that, the encrypted data can only seen by the intended receiver. No, other than the receiver could obtain the data.
- **Imposter prevention:** It includes the elimination of possibility of committing fraud by an imposter.

IV. LITERATURE SURVEY

For securing electronic communication various techniques have been proposed by different researchers. One of the techniques proposed by researchers is a cryptography and steganography for securing data transfer in which images are used as a cover object for steganography and key in for the cryptography [6]. In paper [7], the author describes two step methodologies for hiding secret information based on matching method by using the public steganography. In the first step, by application of Diffie Hellman Key exchange protocol shared stego-key between the two communication parties has been determined (Alice and Bob). In the second step, the stego - key is used by the sender to select pixels which will be used to hide. In paper [8], two approaches have been introduced for securing images of steganography using cryptographic techniques and type conversions. In the first approach, a way to secure the image by converting it into cipher text by using S-DES algorithm with secret key has been proposed. In the second approach, a way of hiding an image in another image by encrypting the image directly through S-DES algorithm via a key image has been explained.In paper [9], a new key symmetric key encryption has been proposed in which both the sender and receiver have the similar key and it should be kept secret in order to make certain an acceptable level of security. In paper [10], a new algorithm with more security SRNN algorithm is based on RSA algorithm has been proposed. This paper explains a new algorithm which achieves high security for digital signature.

In 2012, a novel algorithm for securing electronic communication has been proposed by different researchers. One of the techniques proposed by researchers is a Digital signature algorithm which is based on two hard problems, prime factorization and discrete logarithm [11].In paper [12], Elliptic Curve Digital Signature Algorithm (ECDSA) which is one of the variants of Elliptic Curve Cryptography (ECC) proposed as an alternative to establish public systems such as the Digital Signature Algorithm (DSA) and Rivest Shamir Adleman (RSA), have recently gained a lot of attention in industry and academia.

In 1985, ElGamal Signature Scheme has been described. The ElGamal Scheme is designed particularly for the purpose of signatures, which can be used both as a public-key cryptosystem and a signature scheme. The ElGamal Signature Scheme is non-deterministic, as was the ElGamal Public-key Cryptosystem. This means that there are many geniune signatures for any given message[13]. In 2010, ANSI X9.62 ECDSA over elliptic curve has been implemented. It also discusses related security issues. The main reason for the magnetism of ECDSA is the fact that there is no sub exponential algorithm known to solve the elliptic curve discrete logarithm problem on a properly chosen elliptic curve. In paper [14] the multiple least significant bits (MLSB) steganography, by a pixel trace group model has been analyzed. Based on this model and some statistical characteristics of the images, quantitative steganalysis methods are proposed for two typical MLSB steganography paradigms. A secure and high capacity data hiding technique with blind detection is presented in paper [15]. The image in which the data is embedded has been broken into its constituent bit planes. The data to be embedded in the cover medium has been divided into three variable length data vectors. The data vectors are subsequently embedded in first three ISB planes using a private key generated by Pseudo Random Number Generator (PNRG). In paper [16] cryptography and steganography is combined for improving the security of data. Blowfish Encryption Algorithm is used for encrypting the message to be hidden inside the image for making it non-readable and secure. After encryption, an LSB technique of steganography for enhancing further security is applied. The cryptography and steganography are the two layers of security which makes it difficult to detect the presence of a hidden message.

V. PROPOSED METHODOLOGY

Data security is one of the major concerns which have to be provided for the safe and secure transmission and receiving of data over the network. Cryptography and Steganography plays an important role to provide the security and data hiding to the important data.

In this work, DSA algorithm, is being used which is used to provide secure transaction over the network. This scheme is implemented in a number of networks for the provision of data integrity. The hybrid MLSB scheme is used in this work which is also used to hide the data so that it can never be accessed by any of the hacker or any unauthorized party.

Figure 4 represents the flow of work in a systematic manner. The step 1 is the selection of carrier file which has to be encrypted in order to send it towards the receiving end. This encryption provides the secure and safe transmission to the data which has to be transmitted. The raw data is fetched in the step 2.

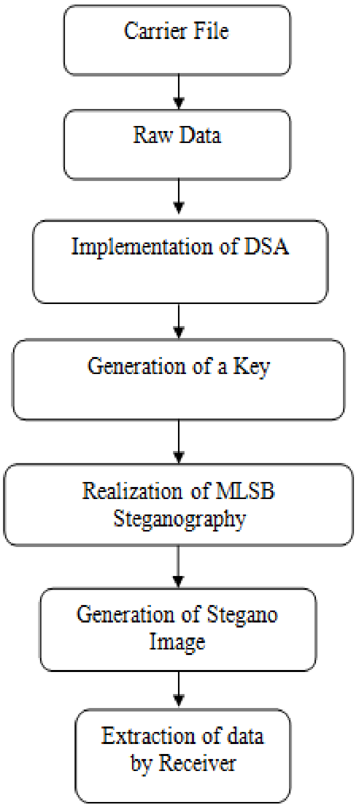
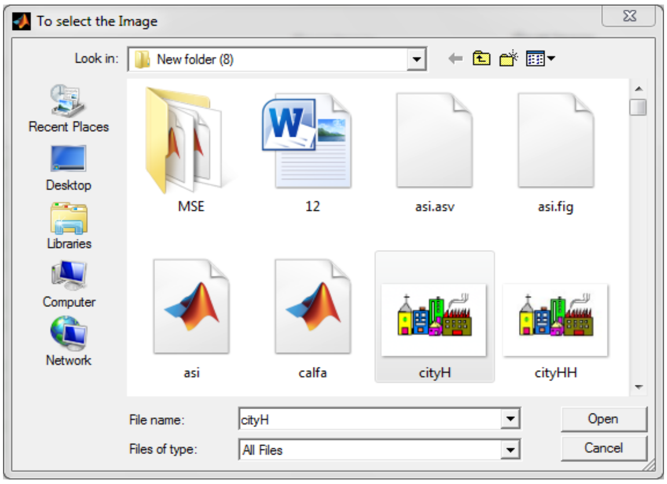

Carrier File
Raw Data
Implementation of DSA
Generation of a Key
Realization of MLSB Steganography
Generation of Stegano Image
Extraction of data by Receiver

Figure 4: Flow of Work

The DSA security algorithm is then provided in the step 3. This algorithm is used to generate a secure key so as to provide the security of the data. Key generation in DSA algorithm, is split up into two steps. The first step is the step where the choice of algorithm parameters is there, which may be shared between dissimilar users within the system, whereas the second step calculates public and private keys for a solitary user. At the step 4, the generation of cryptographic key takes place which is then taken to provide the security to the encrypted data. The data can only be decrypted at the decryption end with the help of this key. The realization of MLSB steganography occurs in step 5. In the last step, the extraction of data is done by the receiver after the generation of Stegano image at step 6

VI. RESULTS AND DISCUSSION

In this section, the simulated results have been carried out by the generation of scenario on MATLAB 7.11. The simulated results show the pictorial representation of outcomes which are explained as follows.



File name: cityH

Files of type: All Files

Figure 5: Selection of Main File

Figure 5 shows the window which is used to select the main file for the purpose to provide the authenticity and security to the broadcasting data. This is the first and one of the major step which is used for the proper and accurate selection of parameters which are then used to provide the secure transmission path to the information which has to be sent over the network.

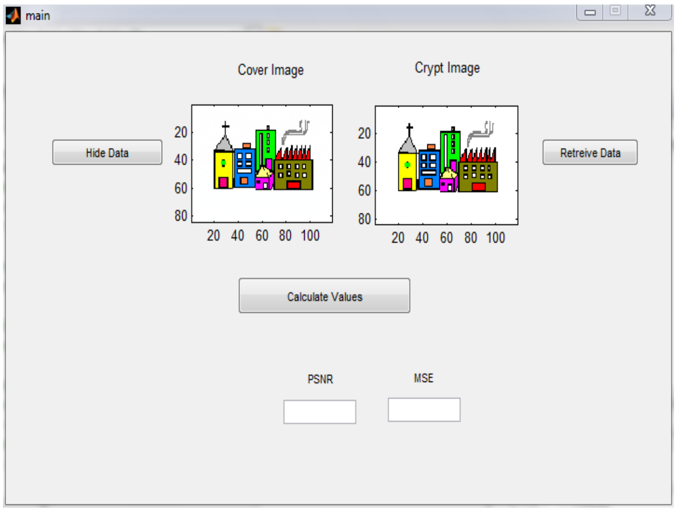
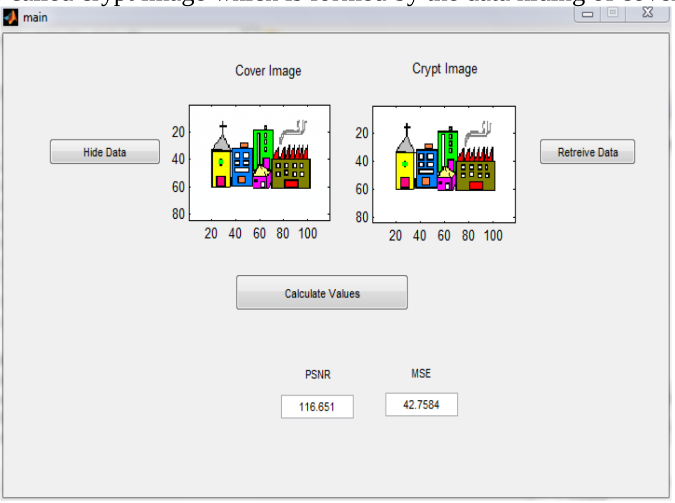


Figure 6: Cover Image and Crypt Image

Figure 6 demonstrates cover image and crypt image. The simple selected file is called cover image and after the encoding of cover image, the data get hidden by the transmitter side in order to provide secure transmission. This image again formed at the receiving end is called crypt image which is formed by the data hiding of cover or real image.



PSNR: 116.651

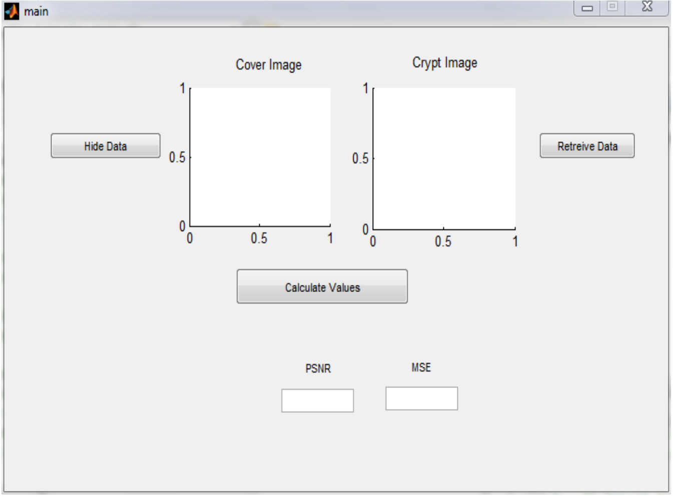
MSE: 42.7584

Figure 7: Values of Cover Image and Crypt Image

Figure 7 shows the values for the cover as well as crypt image. The comparative analysis of the values of cover image and crypt images is shown in the figure 7 where PSNR shows the values of 116.651 and MSE shows 42.7584.

MSE: Mean squared error (MSE) of an estimator measures the average of the "errors", that is, the difference between the estimator and what is estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. The difference occurs because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate. MSE has the same units of measurement as the square of quantity being estimated.

PSNR: Peak signal-to-noise-ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very dynamic range, PSNR is usually expressed in terms of logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g. , for image compression). The signal in that case is the original data, and the noise is the error introduced by the compression. It is most easily defined via the mean squared error (MSE).



.

Figure 8: Graphical Representation of Cover Image and Crypt Image

The graphical representation is represented by figure 7 where the data hiding takes place at cover image and retrieval of data occurs at crypt image. The original data which has to be hidden from the transmission end is then retrieved by the receiver side, i.e. the cover image again gets retrieved by the receiver by using crypt image.

VII. Conclusion

Sending of data over the internet for a variety of reasons has become an essential part of technology now days. Hence, it becomes mandatory to give the protected transmission and receiving of data. For this reason, numerous cryptographic schemes put into practice. In this paper, we have concluded that the Data Hiding Scheme using hybrid Multiple Least Significant bit (MLSB) steganography scheme is one of an effective technique to hide the data which is used along with Digital Signature Scheme Algorithm (DSA). The authentication is done by using DSA technique. The simulator used for the whole process is MATLAB. Hence, in this paper, we have concluded that the proposed DSA algorithm and Data Hiding MLSB schemes provide the better hiding and data security to the data or information sent over the network.

REFERENCES

[1] A. Kahate, *Cryptography and Network Security*, second edition, McGraw-Hill, 2009.

[2] V.K. Pachghare, *Cryptography and information security*. New Delhi, Asoke K. Ghosh, 2009

[3] Dipti, K. S. And Neha, B. 2010. "Proposed System for Data Hiding Using Cryptography and Steganography". *International Journal of computer Appilcations*. 8(9), 7-10, August 2012.

[4] Niels, P. And Peter, H 2003. Hide and Seek: "An Introduction to Steganography". *IEEE Computer Society*. IEEE Security and Privacy, pp. 32-44, May/June 2003

[5] Raphael, A. J., and Sundaram, V. 2011. "Cryptography and Steganography - A Survey". *International Journal of Computer Technology Application*, 2 (3), ISSN: 2229-6093, pp. 626-630.

[6] Domenico, B. And Luca, L. Year., "Image Based Steganography and Cryptography.

[7] C. Oluwakemi Abikoye, S. Kayode Adewole, J Ayotunde Oladipupo, " Efficient Data Hiding System Using Cryptography and Steganography, "*International Journal of Applied Information Systems*, vol. 4, no. 11, 2012.

[8] Sujay, N. and Gaurav, P. 2010., "Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions",.*Signal & Image Processing: An International Journal (SIPIJ)*, 1(2),

[9] Moreeno Ordonez Edward David; Pereira Fábio Dacêncio; Chiaramonte Rodolfo Barros, "VLIW: Cryptoprocessor : Arechitecture and performance in FPGAs," *IJCSNS*, volume 6 no. 8A, 2005.

[10] Mr. Hemant Kumar and Dr.Ajit Singh, "An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography," *IJRREST*, June 2012.

[11] Sushila Vishnoi and Vishal Shrivastava, "A new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem," *International Journal of Computer Trends and Technology*, volume 3, issue 4, 2012.

[12] Aqeel Khalique, Kuldip Singh, Sandeep Sood, "Implementation of Elliptic Curve Digital Signature Algorithm," *International Journal of Computer Applications*, May 2010.

[13] Douglas Stinson, *Cryptography Theory and Practice*, by CRC Press, 1985.

[14] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography,*" Information Forensics and Security, IEEE Transactions,* volume :8, issue :1, Jan 2013.

[15] Shabir A. Parah.,Javaid A. Sheikh. And G.M. Bhat [2] "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique," *International Conference on Emerging Trends in Science, Engineering and Technology,* 2012.

[16] Ajit Singh., Swati Malik, "Securing Data by Using Cryptography with Steganography," *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 3, Issue 5, May 2013.