A Novel Approach for Improving Security by Digital Signature and Image Steganography

Sarika Sharma
Department of Information Technology
IET DAVV
Indore (MP) India

V. Kapoor
Department of Information Technology
IET DAVV
Indore (MP) India

ABSTRACT
Information security is becoming more and more vital with the progress in the exchange of data. Protected communication in the network is a key necessity. Propose a novel technique to encrypt the image and embed the digital signature into the image. A digital signature is a procedure used to certify the authenticity and integrity of a message, software and digital documents. It is a also worn to give testimony of non-repudiation of communications. Steganography is an encryption technique that can be used along with cryptography as more-protected method rising to protect data. Images are the most admired cover objects used for steganography. In the province of digital images lots of different image file formats are present. Java technology proposed to authenticate the performance of the proposed model in circumstances of message length, key length, cipher text length and computational time for encryption and decryption.

General Terms
Image Steganography, Security, Digital Signature, Cryptography

Keywords
Steganography, Security Features, Image, Encryption, Decryption

1. INTRODUCTION
Now a day's internet is used in massive quantities of transmitting the data (i.e. the data are valuable and important). Due to this various type of security attacks feasible for the period of transmission of data over a network. So, several privacy and security issues occur. To keep data from prohibited access there are numerous data security technique like Cryptography, Watermarking, Steganography, data masking, etc. The Cryptography and the Steganography are a traditional approach to secure the data. Cryptography and Steganography are well famous and broadly used modus operandi that organizes information (messages) with the purpose of cipher or obscure their certainty respectively.

The major idea of this scheme is to offer a proficient way to user send or receive messages over a protected channel and ensure the all the key security features. The digital signature is solitary the finest technique to give authentication and non-repudiation and uses a public key algorithm. It uses two keys, one is secret key which is used in favor of signing purpose, and referred to as private key the other is verification key which is open, referred to as public key. Digital signature as well as provide integrity.

Steganography is data veiled in data. Steganography is an encryption method to be used along with cryptography as a more protected scheme where to secure data [18]. Steganography techniques can apply to images, a video file or an audio file. Steganography protects from pirating copyrighted equipment in addition to aiding in illicit aspect. Many different carrier file formats can be used, although image is the most popular [26]. This technique is the most appropriate in favor of encryption that allow a user to cover information within an image. Steganography hides information inside an image so it seems like that no information is hidden in the image [18].

The proposed model ensures the security features like authentication, confidentiality, integrity, availability, non-repudiation. The aim is to offer security via which client transmits their data firmly over channel or internet.

2. LITERATURE REVIEW
The novel approach hybrid technique by Symmetric & Asymmetric key cryptography. This proposal is basically proposed to get better security and sender/receiver simply communicates on protected way [2]. The consistency of a digital signature has to conclude its ability to be used as valid evidence. The predictability of vulnerabilities in technology and the significant probability of an incidence of security threats would build non-repudiation of evidence complicated to accomplish [3].

In recent times, an image clandestine sharing method with steganography and authentication to avert participants from the incidental or intended prerequisite of a false stego-image (an image include the unseen secret image) [4]. In this technique, offered a scheme to get better authentication capability, thus avert lying participants from fraud. The proposed scheme in addition defines the provision of embedded bits to get better features of stego-image [5].

A recent scheme proposed an embedding method which is able to embed a message into an image and achieve minimal image distortion for applications which want a high-visual superiority stego-image. While the alteration of pixels is nominal, applications using the proposed scheme can acquire a stego-image with advanced visual quality than existing studies [6].

A signer can sign a message and affix it with several policies. Only a verifier who gratify the policies attached can verify the authenticity of the message. The belief of policy-controlled signatures resembles a few similarities with nominated verifier signatures, as it can also be used to assign a signature to numerous recipients [7]. Recently, there a new digital signature scheme with shared verification. This scheme is appropriate not barley for digital signatures of one public key, although in addition for situations where multiple public keys are required [8].

In this scheme, illustrate that the self-pairing maps of Lee is not relevant to the recommended applications and that the

signature scheme is yet absolutely broken and presented two cryptographic applications: one is a key agreement scheme furthermore the other is a digital signature scheme [9]. This scheme present secure digital signature as non-repudiation proof, the managing of signature keys turn into the key issue provided that the signature scheme is secure and different approach may be adopted by trusted third parties and common users. Trusted third parties play vital roles in the terms of security services, particularly in non-repudiation services [10].

Steganography is a vibrant tool with the past history and the potential to settle into a new stage of technology. It is the way in which it is used which will resolve whether it is a value or a disservice to our society [11]. This scheme, establish an image steganographic model and include a new high-capacity embedding/extracting component. The key benefit of supporting these two ways is that the sender can apply different technique in different sessions to enlarge obscurity of steganalysis on these stego images [12].

They create the overview of this technique against adaptively chosen message attacks. In a signature scheme, all users distribute a public key while observance for himself a secret key [14]. They widen the security model for authenticated key exchange (AKE) to confine every probable attack resulting from brief and long-term data compromise. It focuses on security form of two-round authentic key exchange (AKE) protocols [15].

Information-hiding techniques in recent times happen to imperative in a numeral of relevant areas. Digital audio, video, and pictures are gradually more furnished amid distinctive, although indiscernible marks, which might contain a hidden copyright notice or serial number or still help to thwart unauthorized copying unswervingly [16]. It describes a variety of approaches of Image Steganography. During examine that there subsist a huge variety of approaches or techniques to defeat secret information in images. The entire technique aims to gratify by three most significant factors of steganographic design, i.e. facility, undetectable, and robustness [17].

In this scheme, anxiety by using the two imperative security mechanisms cryptography and steganography, on sole proposal. To build the information more protected. Today internet has developed into binding in normal life, other than also have concern for protection. To estimate the bit of different steganography algorithms a variety of evaluation parameters are identified based on the superiority of these two algorithms [18].

The role of the cryptography to added wide-ranging issue of trust in an information processing systems. Cryptography can be used to aid with the authentication and, at the destination, to facilitate inflict the policy on conduct received information [19]. They delineate the current activity in developing integrity and security principles based on cryptography. Standard techniques are looked-for accomplishing interoperability and security objectives [20].

They intend a robust authentication scheme among key agreement. Demonstrate that the proposed scheme is secure adjacent to attacks from an antagonist show that rival cannot trail the proposed scheme using at all ways to interrupt the establishment of a common session key [21]. They depict the nature of user authentication along with entity authentication based on the use of cryptographic methods. The receiver of the message can then repeatedly check the existence of this redundancy [22]. They presented a pragmatic study that examines businesses' alleged security concerns with the use of the electronic signature technology for executing contracts and commercial transactions furthermore whether such issues signify a deterrent for their usage [23].

The novel method for secure digital identities under the DSA with a software token with hardware token. During this software token was profitable over PKCS#5 in resisting verifiable text attacks through a hardware (a storage smart card) level security [24]. There are RSA-based constructions of the certificate-less signature scheme. They demonstrate that the idea is provably protected. The scheme is stirred by the zero-knowledge-proof protocol [25]. Enlargement in stealthy communications and steganography will prolong, as will research in building extra robust digital watermarks that can endure image manipulation and attacks. Steganography via itself does not certify secrecy, other than neither does simple encryption. If these methods are collective, nevertheless, stronger encryption methods result [26].

3. RATIONALE

All along, proposed scheme have been talking about the following general scheme:

If follow the first one, that is, when the sender encrypts the message and that encrypted message (i.e. cipher text) compress into the image with the help of image steganography, although this scheme an achieves confidentiality (because the sender's intention to hide the content of the message with the help of Steganography) over the network.

In another scheme, where encrypted message and the digital signature compress into the image by that we can achieve confidentiality, integrity (in case an attacker has access the data and modify it, the digital signature verification at receiver end fails), authentication (identifying and proving the sender's identity), non-repudiation (Sender cannot refuse that they sent the message, as the message was encrypted with their private's key, which is supposed to be known only to sender). That's why we use the second scheme to enhance the security of the system.

4. PROBLEM STATEMENT

In a cryptographic system, the problem is that it cannot accomplish this whole problem in a single step like authentication, confidentiality, integrity, access control and non-repudiation. In an existing scheme the attacker attack on a system simply, brute force attacks easily occur because of the need of security enrichment. Existing system gets more encryption/decryption time because of this our system may do behave badly and generate problems. Hacking is the most important crisis in the existing system. Using proposed methodology we will be enhanced this entire problem.

In a cryptographic system, the point of security of the message is less. To enhance the security you need to achieve all the security of principle in a single step over a system. Proposed system will try to accomplish all the security principles. In cryptography, to securing the cipher text from an attacker is very important then our proposed scheme will securing from the intruder and taking care of the data. In this scheme, proposed model will reduce all the problems which are related to security.

5. PROPOSED METHODOLOGY

In proposed method will try to make sure these entire problem as well as get better system and reliable. The proposed solutions will provide a way to set up secure communication

and it will also facilitate to get the best level of encryption. The system does not need any external system interface for enlargement. A block demonstration of the proposed solution is shown in figure 1.

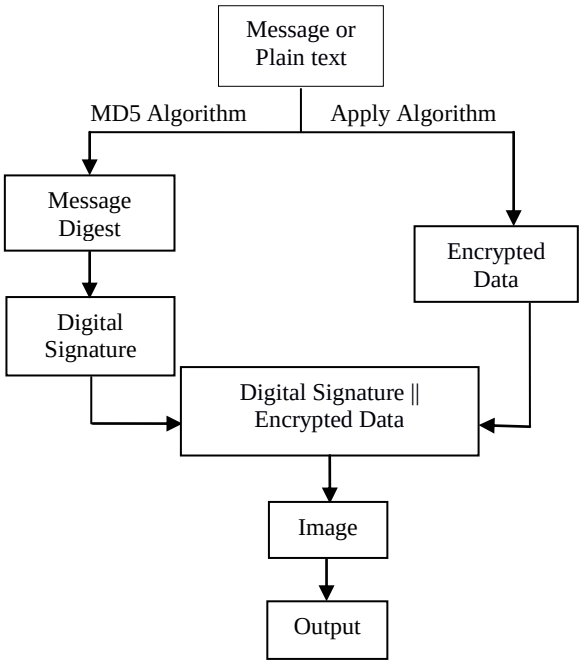

Fig 1: Proposed Scheme

The components of the proposed model are described as:

Plain Text or Message: It is a message which is requisite to secrete, in consequence the proposed scheme, custom the file formats via which the message is formed as input to the system.

Message Digest: The plain text or a message converted into the message digest besides the using of message digest algorithm. A message digest algorithm converts messages into the message digest which is slighter in size.

Digital Signature: The message digest encrypted with the sender's private key and embedded into a digital signature.

Encrypted Data (Or cipher text): It is the produced cipher text after applying RSA algorithm, the data is treated again in this phase. Therefore, initially the whole data are converted into a block.

Digital Signature || Encrypted Data: Now, Digital signature and cipher text are compressed in it an image.

Image: By the using of image steganography compress sensitive data in an image that user wants to share.

Output: Finally, generated image with hidden data which is transmitted in network.

By the help of this scheme, ensure main four security principles that are:

Confidentiality: The sender sends the cipher text and digital signature by the help of image steganography because it hides the existence of the message not everyone knows the hiding information.

Message Authentication: When the verifier validates the digital signature using the public key of a sender, user clinched that the signature has been set apart only by the sender who possess the analogous secret private key and no one else.

Data Integrity: In case an attacker has access to the data and modifies it, the digital signature verification at the receiver end fails.

Non-repudiation: Since it is presumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data.

6. OUTCOMES

The proposed solution will facilitate to enhanced performance, encryption/decryption process, and also improve the security of the system. The proposed methodology is executed using Java technology to approximate the concert of security. The security of information over the internet is flattering a chief concern. The proposed method is used to hide the information in a way that for any prohibited person, it is barely accessible and they cannot easily predictable.

The encrypted digital signature might in the form of the image and by that security may enhance. The intruder will not simply identify it because it is more protected. The major goal of proposed work to build the system protected. After examining the problem, it proposed a security model to get better security paradigms. The acquire result show the confidentiality, integrity, authentication, confidentiality, and non-repudiation. Proposed scheme will make sure that the sender sends the data and this precise data are received by authorized receiver.

7. RESULTS

7.1 Encryption Time

To give further potential concerning the performance of the proposed algorithm, this section talks in excess of the results with different parameters:

Table 1. Encryption Time

File Size (KB)	Encryption Time (ms)	Encryption Space Complexity (KB)
10 KB	120 ms	2910 KB
18 KB	159 ms	3070 KB
32 KB	258 ms	3188 KB
64 KB	315 ms	3269 KB
126 KB	380 ms	3354 KB
250 KB	452 ms	3400 KB

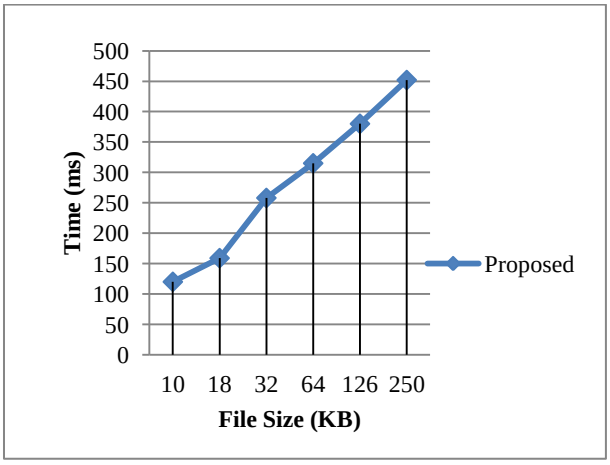

Fig 2: Encryption Time

7.2 Encryption Space Complexity

Space complexity is a gauge of the magnitude of working storage (main memory) an algorithm requires. That means how a lot of memory, in the worst case, is indispensable at some point in the algorithm. Encryption Space Complexity of an algorithm is the overall amount of space consumed by the algorithm in the direction of encrypting the file with respect to the input size.

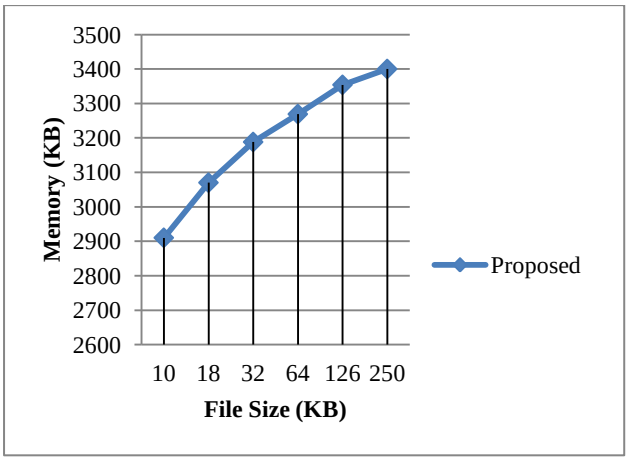

Fig 3: Encryption Space Complexity

7.3 Decryption Time

Decryption is the course of transforming encrypted data yet again in its original form, so it can be understood. The total amount of time required to decrypt the file using the selected algorithm is known as the decryption time.

Table 2. Encryption Time

File Size (KB)	Decryption Time (ms)	Decryption Space Complexity (KB)
10 KB	180 ms	3014 KB
18 KB	215 ms	3146 KB
32 KB	320 ms	3192 KB
64 KB	511 ms	3241 KB
126 KB	572 ms	3296 KB
250 KB	620 ms	3350 KB

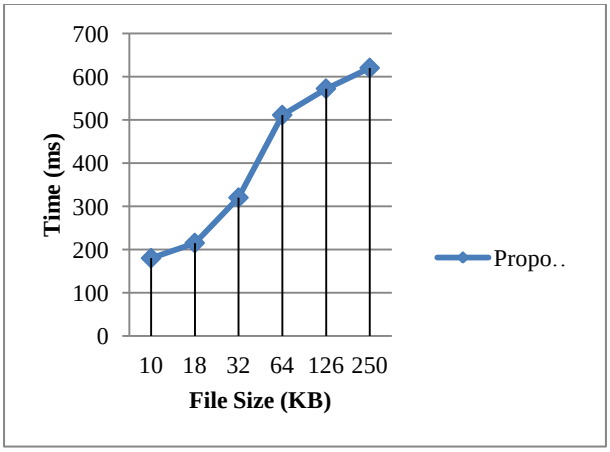

Fig 4: Decryption Time

7.4 Decryption Space Complexity

The total amount of main memory required in the direction of decrypt the encrypted data is known as the decryption memory expenditure or the decryption space complexity. To signify the performance of the system X axis contains the amount of file size used for experimentation and the Y axis shows the amount of main memory consumed in terms of KB (kilobytes).

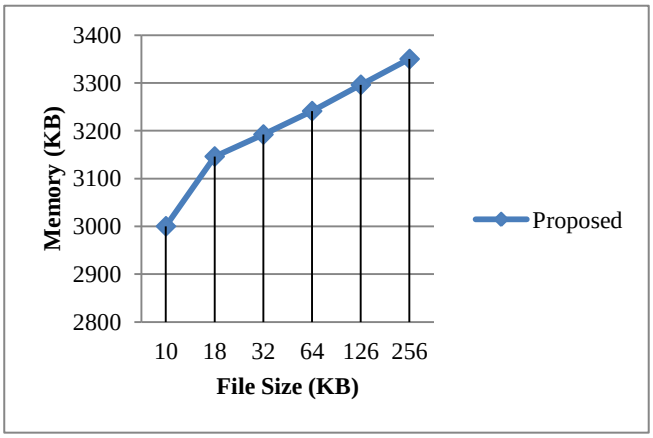

Fig 5: Decryption Space Complexity

7.5 Encryption (Message Estimation)

Table 3. Message Size Estimation (KB)

Plain Text (in KB)	Encrypted Data Size (in KB)
18	616
32	618
64	608
128	700
256	902

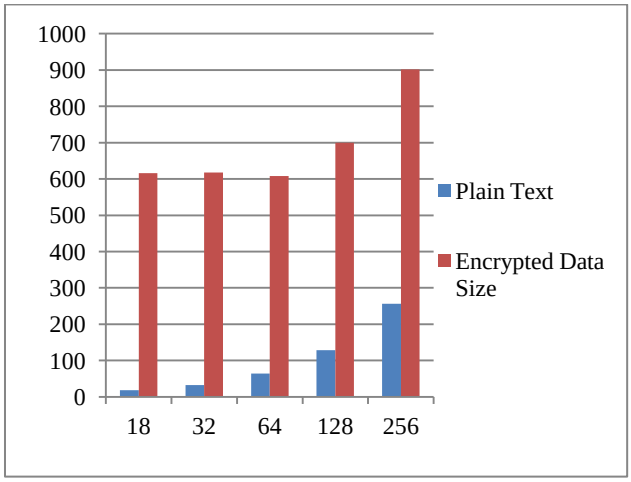

Fig 6: Message Estimation

8. FUTURE WORK

The proposed work is an efficient technique for securing data in unsecured medium. Additional security will formed using these entire features. This is proficient and adaptable in terms of privacy; secure data access and consume less memory. Therefore, the proposed methodology might enhance the system and used in real world application. The security flow is prevented by the attacks happens in this mechanism for that proposed solution must overcome the attacks. Apart from this will centre of attention on the security that there are no probability of attacks or significantly customize image data to make powerful security principles.

9. ACKNOWLEDGMENTS

I would like to say thank you to my guide V. Kapoor for his knowledge and guidance for making this paper a fruitful. We are also grateful to our department of Information Technology for their support.

10. REFERENCES

[1] Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill Publication Company Limited.

[2] Amrita Jain and Vivek Kapoor, "Policy for Secure Communication using Hybrid Encryption Algorithm", International Journal of Computer Application (0975 - 8887) Volume 125 – No. 3, September 2015

[3] Jorge L, Hemandez–Ardieta, Ana I. Gonzalez- Tablas, Jose M. de Fuentes and Benjamin Ramos, "A taxonomy and survey of attacks on digital signatures", Computer & Security, Volume 34, May 2013

[4] Mansi S. Subhedar and Vijay H. Mankar, "Current Status and Key Issues in image steganography: A survey", Computer Science Review, Volumes 13 – 14, November 2014

[5] Ching–Nung Yang, Tse–Shih Chen, Kun Hsuan Yu and Chung–Chun Wang, "Improvements of image sharing with steganography and authentication", Journal of Systems and Software, Volume 80, July 2007.

[6] Ching-Chiuan Lin, "An information hiding scheme with minimal image distortion", Computer Standards & Interfaces, Volume 33, September 2011

[7] Pairat Thorncharoensri, Willy Susilo and Yi Mu, "Policy-controlled signatures and their applications", Computer Standards & Interfaces, August 2016.

[8] Xiao-yun JIA, Shou-shan LUO, Chao-wei YUAN, "A New Signature Scheme with Shared Verification", The Journal of China Universities of Posts and Telecommunications, Volume 13, June 2006.

[9] Je Hong Park, Seongtaek Chee, "A note on digital signature scheme using a self-pairing map", Applied Mathematics and Computation, Volume 169, October 2005.

[10] J. Zhou, K.Y. Lam, "Securing digital signature for non-repudiation", Computer Communications, Volume 22, May 1999.

[11] Silman J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[12] Lee Y.K. and Chen L. H., "High capacity image steganographic model", IEEE Proceedings of Visual Image Signal Processing, Volume 147, 2000.

[13] Menezes, A., van Oorschot, P., and Vanstone, S. 1996. Handbook of Applied Cryptography

[14] David Pointcheval and Jacques Stern, Security proofs for signature schemes, EUROCRYPT '96, Zaragoza, Spain, 1996.

[15] Brain LaMacchia, Kristin lauter and Anton Mityagin, "Strong security of Authentication key Exchange", 2013

[16] Petitcolas, F.A.P., Anderson, R.J. & Kuhn and MG., "Information Hiding – A survey", Proceedings of the IEEE, 87:07, July1999

[17] Priyanka B. Kutade and Parul S. Arora Bhalotra, "A Survey of Various Approaches of Image Steganography", International Journal of Computer Application (0975 - 8887) Volume 109 – No. 3, January 2015.

[18] Manish Trehan and Sumit Mittu, "Steganography and Cryptography Approaches Combined using Medical Digital Images", International Journal of Engineering Research & Technology (IJERT), Volume 4, June 2015

[19] Richard Walton, "Cryptography and trust", Information Security Technical Report, Volume 11, 2006.

[20] Dennis K. Branstad, Miles E. Smid, "Integrity and security standards based on cryptography", Computers & Security, Volume 1, November 1982.

[21] Ren-Chiung Wang, Wen-Shenq Jaung, Chin-Laung Lie, "Robust authentication and key agreement scheme preserving the privacy of secret key", Computer Communications, Volume 34, March 2011

[22] Chris Mitchell, "Authentication using cryptography", Information Security Technical Report, Volume 2, 1997.

[23] A. Srivastava, "Electronic signatures and security issues: An empirical study", Computer Law & Security Review, Volume 25, June 2002

[24] Taekyoung Kwon, "Digital signature algorithm for securing digital identities", Information Processing Letters, Volume 82, June 2002

[25] Jianhong Zhang and Jane Mao, "An effective RSA-based certificateless signature scheme", Journal of Systems and Software, Volume 85, March 2012.

[26] Neil F. Johnson and Sushil Jajodia, "Exploring Steganography: Seeing and Unseen", IEEE Computer, Volume 31, 1998.