A Secure Dual Encryption Scheme Combined With Steganography

A Aswathy Nair[#1], Deepu Job[#2]

[#1] PG Scholar, [#2]Assistant Professor

[#1,#2] Department of Computer Science and Engineering, St. Josephs College of Engineering and Technology Pala, Kottayam

***Abstract*— In this paper a new encoding scheme is proposed which combines encryption and steganography there by ensuring secure data exchange..Encryption hides the confidential information for the purpose of security, by converting the data in to an unintelligible form and steganography hides the data in medias like image, video, audio etc so that the detection of hidden secret is prevented. In the proposed system, the data is dual encrypted and the resultant cipher is then embedded within an image using LSB steganographic technique to ensure secrecy and privacy. The encryption algorithms used is much secure as each step in the process is fully dependent on the key. The LSB steganographic technique hides the data in least significant bits of the pixels of the image and therefore the reflected change in the stego image is hardly noticeable to human eye. The key management for the system is done using RSA encryption technique.**

***Keywords*— Encryption, Steganography, Security, Key-Management.**

I. INTRODUCTION

In today's fast developing era where the people enjoy the most convenient information exchange facilities provided through the highly established electronic medias and internet, there are also certain risk factors. The sensitive information which are transmitted through internet might be intercepted or distorted by unintended observers or hackers by exploiting the weakness for the purpose of destruction or entertainment. So it is of great importance to secure those information which are in transit. There are different mechanisms to ensure the security of the data in transit which includes cryptography, steganography etc.

Cryptography hides the information by transforming it into an unintelligible form, so that one with the possession of the algorithm and key can access the data. This process of transforming the data is termed as encryption. In encryption, using the encryption algorithm and the key, an information content which is termed as the plaintext is transformed into a non readable form. The information content in this form is termed as the cipher text. The encryption key used in the process specifies how the message is to be encoded. The cipher text can be converted back to its original form and the process is termed as decryption. One with the possession of the corresponding decryption algorithm and the key only can retrieve and read the information.

Based on the keys used, the encryption process can be classified as symmetric and asymmetric encryption. In symmetric encryption, same key is used for both encryption and decryption. The sender and receiver have to agree upon this common key, which is used for encryption and decryption process. In the asymmetric encryption, the encryption key of the receiver is published for anyone to use and encrypt messages. This key is known as the public key. However, only the receiving party has access to the decryption key and is capable of reading the encrypted messages. The key which is private to the receiving party is known as the private key.

Steganography conceals the informations within medias in order to prevent hackers from detecting the presence of the secret. It is a process of hiding the message within a media without leaving a remarkable trace. It masks the presence of secret information, making the true message undetectable to the observer. Steganography replaces the bits of unused data in regular computer files with bits of different, invisible information. The information that is hidden within the media can be either plain text, cipher text, or even images. Steganography sometimes is used when encryption is not permitted or is used to supplement encryption. An encrypted file may still hide the information using steganography, so that even if the encrypted file is decrypted, the hidden message is not visible.

There are a large number of steganographic methods ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. There exists many other ways of hiding information like Covert channels, Hidden text within Web pages, Null ciphers etc with computer and networks. Steganography today, allows a user to hide large amounts of information within image or audio files and is there by more sophiscated. These forms of steganography often are used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information and then decrypt it. One of the most widely used

applications of steganography is for so-called digital watermarking. The replication of logo, images, or text on paper stock so that the source of the document can be at least partially authenticated is referred as watermark.

Cryptography converts the secret in to an unintelligible form so that an unauthorized person cannot read the secret. But the existence of the secret is not hidden. An unauthorized person can detect the existence of the secret, but cannot understand it. Since the existence of the secret is detected, they can attempt to capture it through different hacking techniques or can even alter it. Steganography is a technique of hiding the existence of the secret by embedding it in some media like image, audio, video etc. It does not modify or convert the secret, but only hides its existence. Security can be enhanced on combining steganography with cryptography so that the secret which is converted in to a non readable form is embedded in to some media to hide the existence of the secret. Most systems that exist today use steganography or cryptography alone to ensure the confidentiality of the message and some of them combines both to enhance the security. Certain systems embed the secret within some media and then convert the resultant media in to cipher. This approach enhances the security, but the purpose of steganography is not used here.

In this paper a new secure scheme is proposed which includes a combination of cryptography and steganography to achieve data privacy over secrecy there by increasing the security. It is used to securely exchange confidential informations between organizations. The enhanced security feature is attained through two steps of encryption and a final step of steganography. The message that is to be transmitted is first converted in to a cipher image through the first encryption process. The cipher image is then converted in to an intermediate text through the second encryption process. The intermediate cipher text generated is then hidden within a cover image using steganography to hide the existence of the secret and this resultant stego image is transmitted to the receiver through the network. Thus through this process a high degree of security for information is achieved.

II. Related work

Cryptography hides information by transforming it to an un intelligible form. It is used in technologically advanced applications, which includes areas such as the security of ATM cards, passwords, and e-commerce, which all depend on cryptography. Steganography is a method of hiding information in ways that prevent the detection of hidden messages. The majority of steganographic systems that exists today uses multimedia objects like image, audio, video etc as the cover to hide the message, because people often transmit digital pictures over email and other Internet communication. Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message in way that it is converted in to an unintelligible form.. Steganography embeds the message with in any media, so that it is hidden. More often in today's security advancement, there exists certain cases in which a combination of Cryptography and Steganography are used to achieve data privacy over secrecy. Different software tools are also available in this regard.

Thomas Leontin Philjon et al. [4] proposed a system in which the cryptography is combined with steganography to enhance security of the message to be send. First the message to be send is encrypted to generate a cipher. image. The cipher image is then embedded in to the cover image to generate the intermediate text. The same encryption technique is repeated on the intermediate text to generate the cipher image. This cipher image is then send to the recipient. At the receiver side, the received cipher image is decrypted to generate the intermediate text. From the intermediate text and using the cover image, the cipher image is extracted. The message is then obtained by decrypting the cipher image and using the cover image as the key. This method enhances the security of the message , but the existence of the message is not hidden since encryption is done after steganography and the cipher image is send to the recipient. The cipher image is a distorted image which reveals the existence of the secret.

Hikmat Farhat et al[5] suggests two methods to improve steganographic techniques. In the first approach steganography is combined with cryptography to make it harder for a steganalyst to retrieve the plaintext of a secret message from a stego-object. Here both the sender and the recipient agree on a cover image to send a secret message. The protocol does not modify the cover image, rather it determines the bits of the secret message that match the ones in the cover image and stores their different locations in a vector. This vector is then sent to the recipient. This approach is much secure, but once the hacker obtains the cover image then the message can be retrieved easily. In the second approach, a secret message is hidden in more than one cover object. The secret message is divided into as many parts as the number of cover images and each part is hidden in one of the cover image. The greater the number of cover images, the harder it will be for a steganalyst to retrieve the message. Here the sender and recipient has to agree upon a particular algorithm and exchange all the cover images and the stego images. This method is not feasible as the number of cover image increases.

Dhawal Seth, et al[6] proposes a combination of encryption and steganography to enhance the security of the data to be sent. First the message is encrypted using DES algorithm and the resultant cipher message is then embedded into a cover image using LSB algorithm. This is a secure approach to send message as the message is encrypted and the existence of the message is hidden using steganography. But DES algorithm has several weakness. The size of the key used in DES is 56 bit and the possible number of key is 256 . Therefore brute force key search can be done by trying every possible key in order to recover the plaintext. Also cryptanalysis can be done on different cipher text to find the keys as some internal structures used in DES are not designed to be strong against linear cryptanalysis. So if the existence of the

message is detected, then it will not be difficult for a cryptanalyst to retrieve the message. Therefore this approach cannot be used for critical situations.

Shouchao Song, et al[7] proposed a new secure communication protocol that combines steganography and cryptography techniques. It is based on the LSB matching method and the well-developed Boolean functions in stream ciphers. The Boolean function is used for encryption and controlling the pseudo-random increment or decrement of LSB. This approach accomplish both the encryption and steganography in one stop and therefore require less computation while maintaining high secure quality. The drawback of this approach is that it focuses only on gray scale cover image and is not suitable for other types of images.

Paruchuri, et al. [8] proposed a system in which steganography is combined with cryptography to enhance security. First the message to be send is embedded in to a cover image using steganography and the stego image is encrypted to produce the cipher image. The cipher image is then send to the recipient. This approach is a secure, but the existence of the message is not hidden since encryption is done after steganography and the cipher image is send to the recipient. The cipher image does not resemble the cover image and will be distorted.

III. Proposed System

In this paper, we present a more secure message transmission scheme using double encryption and steganography. At the sender side, first the message to be transmitted is encrypted using angular encryption algorithm which converts the message to a cipher image. The key used for this encryption is a cover image and a random point P(x,y) of the cover image. The cipher image is generated by combining the message with the cover image using the input point. The resultant cipher image is then encrypted using metamorphic algorithm and an intermediate text is generated. The key used for metamorphic encryption algorithm is the cover image and the resultant cipher text is generated by combining the two images. The resultant cipher text is then hidden within the cover image using LSB steganography and a secret text as the key where the key and the cipher is embedded in the least significant bits of the image pixels. The key management is done using RSA encryption algorithm. The point and the secret text is encrypted using the RSA algorithm and transmitted to the recipient.

A. Angular Encryption

Angular encryption algorithm accepts the confidential message M, a cover image and a random point P(x,y) on the image as input. The three consecutive characters of the messages are embedded in the R,G and B value of a single pixel. Therefore the steps from 2.1 to 2.11 in the algorithm is repeated one by third times the number of characters in the message. The angle θ is computed as the angle between

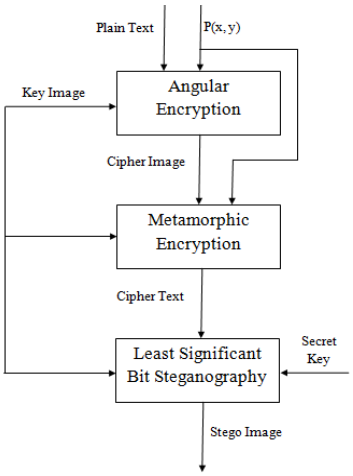

Fig1 : Block Diagram For Encryption Combined with Steganography

the line P(x,y) C(x,y) and the line from perpendicular to the line P(x,y) C(x,y) to the point C(x,y) as shown in figure1. Hence θ can be computed as cos inverse of (P(x)-C(x)) / d.

The ASCII value of each of the three consecutive characters are XORed with 'd' which is the distance between P(x,y) and C(x',y') and is then left shifted θ times. Then the resultant three 8-bit values are XORed respectively with the R,G and B value of a random pixel from the key image and the resultant is set in the cipher image.

Algorithm Angular Encryption

Input: Secret Message(M), Key Image, P(x,y)
Output: Cipher Image

1. Compute n as (length of M) / 3
2. For i ranging from 0 to n
   - 2.1 Find the pixel to be set in the cipher as C(x,y)
     Where x = i % (width of key image)
     y = i / (width of key image)
   - 2.2 Calculate θ = angle between C(x,y)and P(x, y)
   - 2.3 Calculate d = number of pixels between the C(x,y) and P(x, y).
   - 2.4 Compute ASCII value of the three consecutive characters from position i.
   - 2.5 XOR the ASCII values with d
   - 2.6 Shift the resultant 8-bit binary values θ times to the left
   - 2.7 Compute x1= 13*(i+p(x)+x1) and y1= x1+p(y)
   - 2.8 If p'(x1,y1) is within the key image get rgb value of the point p'(x1,y1) from the cover image
   - 2.9 Else set x1= (width of key image) / 3 and get the rgb value
   - 2.10 XOR the rgb value with the value obtained from step 2.6
   - 2.11 Set the resultant value in the cipher image
3. Obtain the complete cipher image

End Angular Encryption

B. Metamorphic Encryption

The cover image, a point on cover image and the cipher image which is the output of the angular encryption algorithm is combined and an intermediate cipher text is generated. The R, G and B value of each pixel in the cipher image is XORed with the R, G and B value of random pixels computed using P(x,y) in the cover image. The resultant 8-bit values are split

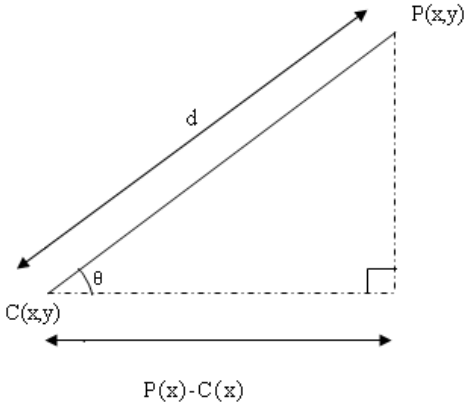

Fig2: Angle Computation

in to 4 bit values and are assigned characters based on the Table 1. The characters are assigned depending on 4-bit value and the category they belong, ie whether it belongs to R, G or B component of the pixel.

Algorithm Metamorphic Encryption

Input: Cipher image, Key image, P(x, y)
Output: Cipher text

1. For every pixel in the cipher image
   1.1 Split the pixel into its R, G, B values.
   1.2 Compute x1= 7*(i + p(x) +x1) and y1= x1+p(y)
   1.3 If p'(x1, y1) is within the key image get rgb value of the point p'(x1,y1) from the cover image
   1.4 Else set x1= (width of key image) / 3 and get the rgb value
   1.5 Perform exclusive OR operation on R, G and B value of the cipher image with the respective R, G and B value of the random pixel
   1.6 Split the resultant 8-bit value in to 4-bit values and assign characters based on Table
2. Combine all the characters and obtain the cipher text

End Metamorphic Encryption

C. LSB Steganography Encoding

The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images can be 24 bit or 8 bit. In 24 bit images three bits of information can be embedded in each pixel, one in each of the LSB position of the three eight bit LSB values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image and hence cover image resembles with the stego image. In 8 bit images, one bit of information can be hidden. The input for the algorithm is the cover image, cipher text and secret key. The secret key followed by the length of the cipher text is embedded in the least significant part of the RGB values of each pixel of the cover image. Finally the cipher text is embedded in the cover image.

TABLE I

CHARACTER ENCODING TABLE

	R	G	B
0000	Q	w	E
0001	r	T	y
0010	Z	x	C
0011	v	B	n
0100	M	u	I
0101	O	p	L
0110	K	j	H
0111	g	F	d
1000	S	a	m
1001	N	b	V
1010	c	X	z
1011	P	i	o
1100	e	q	W
1101	Y	R	t
1110	A	s	D
1111	f	G	h

Algorithm LSB Steganography Encoding

Input: Cipher Text, Secret Key, Cover Image
Output: Stego Image

1 Compute 256 bit hash of the secret key and represent as thirty two 8 bit values
2 For i ranging from 1 to 32
   1.1 Select the pixel in the cover image to embed the hash
   1.2 Split the pixel in to RGB values
   1.3 Embed the hash in to LSB part of the R, G and B values of the pixel

3 Represent message length as 32 bits
4 For i ranging from 1 to 4
   4.1 Select the pixel in the cover image to embed the hash
   4.2 Split the pixel in to RGB values
   4.3 Embed the message length in to LSB part of the R, G and B values of the pixel

5 For i ranging from 1 to length of cipher text
   5.1 Select the pixel in the cover image to embed the cipher text
   5.2 Split the pixel in to RGB values
   5.3 Embed the cipher text in to LSB part of the R, G and B values of the pixel

End LSB steganography

Thus the overall processes at the sender side include dual encryption and steganography. The input secret message is first converted to a cipher image using key image and the p(x, y) through angular encryption process. The

cipher image is again encrypted to generate the intermediate text through metamorphic encryption process. Finally the intermediate text is embedded within the key image using LSB steganography and the stego image is send to the recipient.

Algorithm Text Encoding

Input: Secret Message(M), Key Image(KI), P(x, y), Secret Key(K)
Output: Stego Image

1 Get the secret message
2 Cipher_image(CI)=Angular_Encryption{M,KI,P(x, y)}
3 Cipher_Text(CM)=Metamorphic_Encryption{CI,KI, P(x, y)}
4 Stego Image= LSB_Steganography{CM, KI, K}

End Text Encoding

At the recipient side, the stego image is processed to retrieve the cipher text using the LSB algorithm. The cipher text is then decrypted using the metamorphic decryption algorithm to retrieve the cipher image. The resultant cipher image is decrypted to generate the confidential message using the angular decryption algorithm. The series of steps for decoding the message at the recipients side is as shown in figure 3.

D. LSB Steganography Decoding

The input to the LSB decoding process is the secret key, cover image and the stego image. The secret key embedded in the stego image is extracted from the pixels by comparing with the pixels of the cover image and length of the input secret key .The extracted secret key is compared with the input key. If it matches then the length of the message followed by the cipher text is extracted.

Algorithm LSB Steganography Decoding
Input: Stego Image, Secret Key, Cover Image
Output: Cipher Text

1. Compute 256 bit hash of the secret key and represent as thirty two 8bit value
2. For i ranging from 1 to 8
   - 2.1 Select the pixel in the stego image to extract the secret key comparing with the cover image
   - 2.2 Split the pixel in to RGB values
   - 2.3 Extract the secret key character from the LSB part of the R, G and B values of the pixel
3. For i ranging from 1 to 4
   - 3.1 Select the pixel in the stego image by comparing with the cover image
   - 3.2 Split the pixel in to RGB values
   - 3.3 Retrieve the message length from LSB part of the R, G and B values of the pixel
4. For i ranging from 1 to length of cipher text
   - 4.1 Select the pixel in the stego image to extract the secret key comparing with the cover image
   - 4.2 Split the pixel in to RGB values
   - 4.3 Extract the cipher text character from the LSB part of the R,G and B values of the pixel
   - 4.4 Increment value of i by 3

End LSB Steganography Decoding

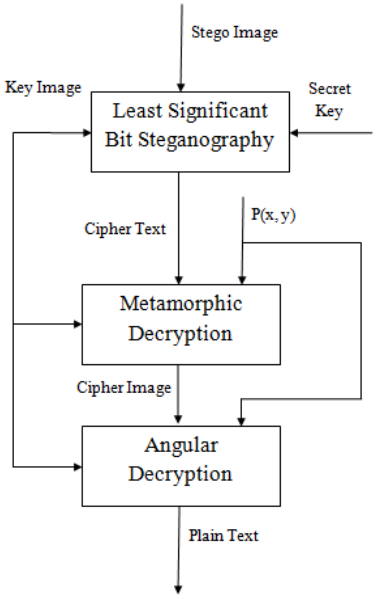

Fig 3: Block Diagram For Decoding of Message

E. Metamorphic Decryption

The decryption process generates the cipher image from the cover image and intermediate text using the key point on the cover image and Table 1. The pixel from the cover image is selected using P(x, y) and is splited in to R,G and B values. The value of the characters obtained from Table 1 is XORed with the respective values of the pixel to generate the pixel of the cipher. This process is repeated for the entire characters of the intermediate text.

Message:

meet me on sunday at 4:00 pm

Cipher Image:

Cipher Text:

KqsOhlRRabInfpWwilcgWxlhNZWFhDAqOWYhScwBh
eSZxPdIrvFPCngqwjEz

Fig4 : Secret message, cipher image and cipher text

Algorithm Metamorphic Decryption

Input: Cipher text, Key image, P(x, y)
Output: Cipher image

1. Compute width of cipher image as length of the cipher text divided by 6
2. For i ranging from 1 to width of cipher image
   2.1 Compute x1= 7*(i+ p(x)+x1) and y1= x1 +p(y)
   2.2 If p'(x1,y1) is within the cover image get rgb value of the point p'(x1,y1) from the cover image
   2.3 Else set x1= (width of key image) / 3 and get the rgb value
   2.4 Perform exclusive OR operation on corresponding value of the character obtained from table with the respective R, G and B value of the random pixel
   2.5 Set the pixel in the cipher image
3. Obtain the complete cipher image

End Metamorphic Decryption

Fig 5(a): Original Cover Image

F. Angular Decryption

The confidential message is retrieved from the cipher image by angular decryption process. The R, G and B value of the pixels in the cipher image is retrieved and exclusive OR operation is performed with corresponding R, G and B value

Fig 5(b): Stego image after encoding

of the random points on the key image obtained from P(x, y). Compute angle θ and distance d as in encryption process. The resultant is then right shifted θ times, which is again XORed with the distance d . The 8-bit value obtained is the ASCII value of the text message and by encoding them to character values and combining the plain text is generated.

Algorithm Angular Decryption

Input: Cipher Image , Key Image, P(x,y)
Output: Secret Message(M)

1. Compute n as width of cipher image
2. For i ranging from 0 to n
   2.1Compute x1= 13*(i+p(x)+x1) and y1=x1+p(y)
   2.2 If p'(x1,y1) is within the key image get rgb value of the point p'(x1,y1) from the cover image
   2.3 Else set x1= (width of key image) / 3 and get the rgb value
   2.4 Obtain the rgb value of the pixel p'(i, 0) in the cipher image and XOR it with the rgb value obtained from step 2.3

   2.5 Find the point in the key image C(x,y)
   Where x = i % (width of key image)
   y = i / (width of key image)
   2.6 Calculate θ = angle between C(x,y)and P(x, y)
   2.7 Calculate d = number of pixels between the C(x,y) and P(x, y).
   2.8 Right shift the resultant from step 2.4 θ times and XOR each with d
   2.9 The resultant is the ASCII value of the character in the secret message and encode to respective characters

3. Combine the characters to obtain the complete message

End Angular Decryption

The overall process at the receiver's side include the decoding of the secret message from the stego image. First the cipher text is decoded from the stego image using LSB steganography decoding process. The resultant cipher text is decrypted using metamorphic encryption to generate the cipher image. The secret message is then decoded from the cipher image using angular encryption.

Algorithm Text Decoding

Input: Stego Image(SI), Key Image(KI), P(x, y), Secret Key(K)
Output: Secret Message(M)

1 Get the secret message
2 Cipher_Text(CM)=LSB_Steganography{SI, KI, K}
3 Cipher_image(CI)=Metamorphic_Decryption{CM,KI, P(x, y)}
4 Secret Message(M)=Angular_Decryption{CI,KI,P(x, y)
End Text Decoding

G. Key Management

The cover image, a point on the cover image and a secret key are the keys used to encrypt and embed the confidential message within the cover image. The secret key and the point on the cover image is concatenated and encrypted using RSA encryption algorithm. The keys are encrypted using the receiver's public key and the resultant cipher can be transmitted to the receiver along with the cover image. At the receiver's side the key can be decrypted using the private key of the receiver. The resultant is then separated and can be used for extracting the confidential message.

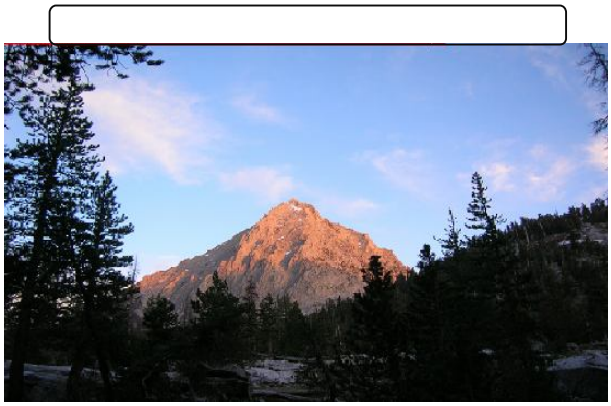

Fig 6: Stego Image with encoded portion marked

IV. Implementation and Results

The proposed system was implemented in core java for png images and MySQL is used as the database. The users can transmit messages securely and efficiently through the system. Since the message is dual encrypted, which converts the message to image and then to cipher text, there is no chance of retrieving the message from the cipher. The encryption technique is also efficient since each step of the process is fully dependent on the key. The message is encoded in ASCII encodings and has undergone a series of shift operations and exclusive OR operations. The resultant is then performed exclusive OR operation with the random pixels of the cover image and the cipher image is generated. The random pixel is selected based on the input point p(x, y) of the cover image. The shift operation is performed 'θ' times where θ varies after each interval of 3 characters. The exclusive OR operation is done with the distance 'd', which also varies at the same interval. The cipher image is then combined with the random pixels of the cover image and cipher text is generated based on the table. The table is designed in such a way that the pixel is divided in to R, G and B values of 8-bit each and these values are splitted to two 4-bit values. Each of these 4-bit values are assigned unique characters based on whether it belongs to R, G or B component.

The message and its conversion to cipher image and cipher text, as the result of dual encryption is as in figure 4. Since the existence of the secret is hidden by embedding it in the cover image, there is lesser chance of attempts to get the secret. The LSB steganographic algorithm is used for embedding the cipher within the cover image. Selected pixels of the cover image is split in to 8-bit R, G and B values and the last 4 bits of each of the values is flipped to reflect the message. Therefore the difference between the cover image and the stego image is hardly noticeable to the human eye as shown in figure 5. In addition to the cipher text, the secret key and the length of the cipher is also embedded before the cipher text in to the cover image. Therefore one with the possession of the secret key can only get the cipher text embedded in the image. The portion of the cover image that is used for embedding a message of length 100 characters is as indicated by the red marking in figure 6. The keys used for the encoding process is the cover image, the point p(x, y) on the cover image and the secret key. The secret key can be of any length since the hash of the key is used for encoding.

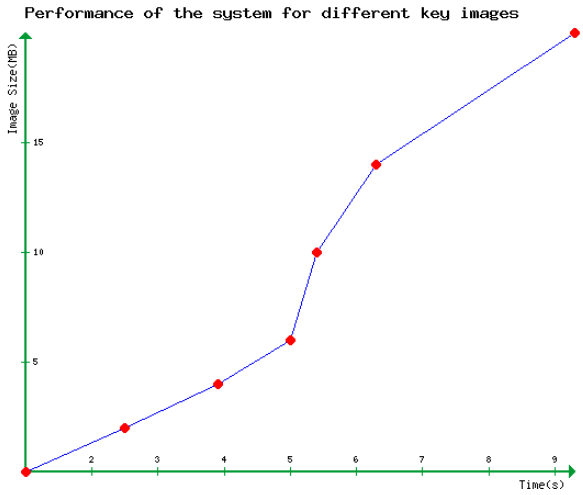

Fig 7: Performance of the system for different key images

The secret key and the point p(x, y) is concatenated and is encrypted using RSA encryption algorithm. The resultant cipher of the RSA algorithm and the cover image is transmitted to the receiver through e-mail. Since the secret key and the point is encrypted using the receivers public key, it can be decrypted only by the intended receiver. One with the possession of the cover image and the stego image cannot extract the message without the point and the secret key. The time required for encoding and decoding process varies depending on the size of the image and only slightly varies with the number of characters in the message. The performance of the system was tested for different sized images, keeping the character length constant. Figure 7 indicates the variation of encoding time with the size of the key image for an input of three hundred characters. The system was also tested with different plain text character length and the result analysis proved that the time taken for encoding is almost constant with the increase in character count. The proposed system works efficiently even for more than thousand characters, provided the key image is larger in size depending on the number of characters.

V. CONCLUSIONS

In this paper a secure and efficient encoding system was proposed which include dual encryption and steganography. The dual encryption provides better security since each step of the encryption process fully depends on the key. The resultant cipher is embedded within the key image which prevents the detection of the secret. LSB steganographic technique is used for the embedding of the image and therefore the reflected change in the stego image is hardly noticeable to human eye. Efficient key management is achieved by encrypting the key using RSA encryption technique. The system was successfully implemented and tested. The performance of the system is also plotted based on the result analysis.

REFERENCES

[1] T. Sharp. An implementation of key-based digital signal steganography. *Proc. 4th. Information Hiding Workshop*, LNCS, vol. 2137, Berlin: Springer-Verlag, 2001, pp. 13–26.

[2] Westfeld A, Pfitzmann A. Attacks on Steganographic Systems, *Proc. 3rd. Information Hiding Workshop*, LNCS,Vol.1768,Berlin: Springer-Verlag, 2000, pp.61-76

[3] Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and gray-scale images. *IEEE Multimedia*, 2001, Vol.8(4),pp.22-28.

[4] Thomas Leontin Philjon. and Venkateshvara Rao. —"*Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption*" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011

[5] Khalil Challita and Hikmat Farhat ,"*Combining Steganography and Cryptography: New Directions*", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208,The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).

[6] Dhawal Seth, L. Ramanathan,"*SecurityEnhancement: Combining Cryptography and Steganography*", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010.

[7] Shouchao Song, Jie Zhangb,Xin Liao,Jiao Du Qiaoyan Wen, "*A Novel Secure Communication Protocol Combining Steganography and Cryptography*"**,** 2011 Published by Elsevier Ltd. Selection and/or peerunder responsibility of [CEIS 2011] In Advanced in Control Engineering and Information Science.

[8] Dr.R.Sridevi,Vijaya, Paruchuri,,K.S.SadaShiva Rao, "*Image Steganography combined with Cryptography* ",Council for Innovative Research Peer Review Research Publishing System Journal: IJCT Vol 9, No 1 , ISSN 22773061 976 | P a g e J u l y 1 5 , 2 0 1 3 editor@cirworld.com

[9] "Cryptography and Network Security: principles and practices", William Stallings, pearsons education, first Indian reprint 2003.

[10] Johnson, Neil F., and SushilJajodia. "Exploring Steganography: Seeing the Unseen", IEEE Computer Feb. 1998: 26-34.

[11] Rosziati Ibrahim and Teoh Suk Kuan —Steganography Algorithm to Hide Secret Message inside an Image‖ Computer Technology and Application 2 (2011) 102-108

[12] Diffie W and Hellman M, "New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22(6): 644-654, 1976

[13] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana —A Competitive Study of Cryptography Techniques over Block Cipher‖ UKSim 13th IEEE International Conference on Modelling and Simulation 2011

[14] Wenbo Mao. Modern cryptography: Theory and practice. *Prentic Hall, 1st edition*, 2003.

[15] D. Gruhl, W. Bender, and N. Morimoto, "Techniques for data hiding," Tech. rep., MIT Media Lab, Cambridge, MA, 1994.

[16] Nath A., Ghosh S., Mallik M.A., "Symmetric Key Cryptography Using Random Key Generator", Proceedings of the 2010 International Conference on Security & Management, SAM-2010, Vol. 2, pp. 239-244, Las Vegas Nevada (USA), 12-15 July 2010.

[17] Al-Fayoumi,Aboud Jabbar.H "*An Efficient RSA Public Key Encryption Scheme*" Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on DOI: 10.1109/ITNG.2008.199 2008 , Page(s): 127- 130