Journal of Multidisciplinary Engineering Science Studies (JMESS)
ISSN: 2458-925X
Vol. 3 Issue 2, February - 2017

A Novel Two Layer of Security by Using Cryptography along with Steganography

Sajid Khan
Department of Computer Sciences
Preston University Kohat
Islamabad, Pakistan
Khansajid_te66@yahoo.com

Dr. Malik Sikander Hayat Khiyal
Faculty of computer science
Preston University Kohat
Islamabad, Pakistan
m.sikandarhayat@yahoo.com

***Abstract*— Security of data is an important task till from the beginning of internet to the current era. Currently main concern is over the transmitting of sensitive or high value data through open or non-secure channel to the destination point in such a way that neither confidentiality nor the integrity of data has to be compromised. Conversion of actual information into some scrawled arrangement is termed as encryption. Although widely used cryptography techniques are still in use but alone it is not capable of protecting and hiding of data proficiently. Eavesdropper or detective can certainly identify the presence of scrambled information and can attempt a few cryptanalyses tactics to get the original information. So to enrich the safety of data a new approach is proposed that provides an easy to implementable and better security. The proposed work is about encrypting the plain text message by Rivest Cipher 4 (RC4) algorithm and then hiding the message into an image through steganography. Encryption has done in the 1st step while in the 2nd step pixel replacing by using k-modulus method has been used for image hiding.**

Keywords— steganography, cryptography, cipher text, encoding, image hiding, stego-image, k-modulus method.

I. INTRODUCTION

In current era of communication, one of the compulsory requirements to thwart data stealing is safeguarding the data. Safety has become a serious article for prosperous and almost all other related networks. Different techniques are used from the beginning for this purpose [1]. Basically cryptography came from Greek kryptos, "hidden", plus graphein, "to write", means learning of transforming evidence from its customary understandable format into an unintelligible form, representing untidy deprived of secret key is called encryption [2]. Understandable form of data is called plain data or simple text [3]. Encrypted info can occasionally be cracked by hackers or code breakers, though recent cryptography methods are almost resilient. The general procedure of encryption and decryption is presented in Fig. 1.

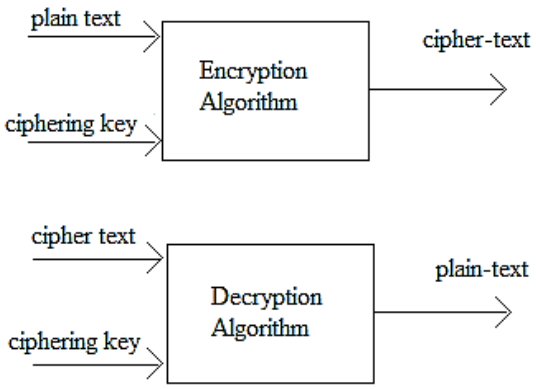


Fig.1: The Process of Encryption and Decryption

Encryption algorithms have two types: one is symmetric and the second is asymmetric. In the first type despatcher and recipient will have the identical key for the purpose of encoding and decoding of message while in the second type instead of same public and private keys, two different keys are used for encoding and decoding at sender and receiver site respectively. Well known symmetric and asymmetric algorithms are as follows [4].

Well known symmetric algorithms are:

- Data Encryption Standard (DES)
- Advance Encryption Standard (AES)
- Two-fish & Blowfish
- Triple Data Encryption Algorithm (TDEA)

Few asymmetric algorithms :

- Diffie–Hellman–Merkle (D-H)
- Ron Rivest, Adi Shamir, Leonard Adleman (RSA)
- Digital Signature Algorithm (DSA)

To overcome the limitations of cryptographic methods, a new technique of steganography has been introduced as an innovative way of secret communication in modern era. It delivers information by covertly implanting into shelter medium using some info hiding methods [5].

Both steganography and cryptography are the two significant divisions of data safekeeping. Cryptography delivers encryption practices for a safe communication. Cryptography can be recalled as an art of science in

which scientific methods are used for possession message safe and free from attackers [6, 7] while steganography is a branch of science that envelop the existence of information [8].

Generally Steganography can be alienated into five different categories [9], text steganography, image steganography, audio steganography, video steganography and protocol steganography. These all have subtypes too. The general illustration of steganography is shown in Fig. 2.

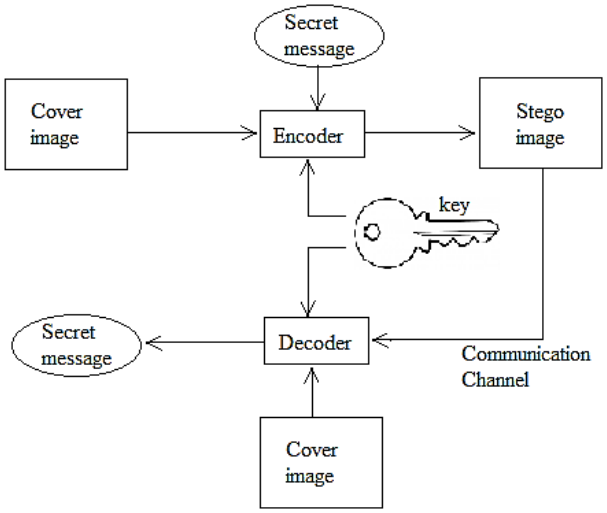


Fig. 2: General Block Diagram of Steganography [10]

II. Literature Review

Cryptography and digital steganography methods are commonly used to avert and exasperate foe's attacks from illicit access. Different integrated forms of steganography and cryptography proposed with the passage of time [11].

The authors in [12] have used a combination of DES technique of cryptography with LSB. In this technique encryption of data was done by DES and then that cipher text hided inside a cover carrier which was an image. The insertion process is accomplished by using LSB steganography. The cipher text is first transformed into binary then least significant bit of cover image is substituted with the binary encrypted text. The main hindrances associated with LSB method is that the interloper can alter the least significant bit of all the image pixels and the information gets destroyed. This scheme cannot abide image compression and noise.

In [13] the author used an integrated technique of AES and DCT. Cipher text was generated from the plain text using AES encryption and then embedded into the concealment image by using DCT based steganography. The DCT transformation is applied over the cover image so that it could get separated into low, high and middle frequency gears. The main issue associated with this method is as the size of data increases image quality decreases.

In [14] the authors proposed a novel technique, which was the combination of DWT based steganography along with AES encryption. In this technique AES algorithm is used to generate encrypted text. The encrypted text, then incorporated the cover image using DWT, based on which a transformation DWT is applied for cover images. But it has larger compression time, lower quality than JPEG at low compression rate. Also the use of larger DWT function produces distorting and ringing noise near edge regions in images.

The authors in [15] proposed a technique of AES combine with LSB. For encryption of data AES algorithm was used and then that encrypted text was entrenched into an image. The image used as a carrier was 24 bit. But LSB insertion is very susceptible to a lot of alterations also a lossy compression, e.g. JPEG, is very likely to abolish it absolutely.

AES along with DCT steganography with cipher text splitting, in this combination for the purpose to decrease the bulk of data entrenched in an image it embed solitary a chunk of the cipher text. AES encryption technique was used to convert the plain text an unreadable. After that, the cipher text was splinted before it embedded directly into the cover image [16]. The main downside of the system is it uses two extra keys which are very large compared to the part of data embedded in the cover image, so key exchange could be exorbitant.

III. Proposed Technique

Matrix Laboratory (MATLAB) programming language is used as a tool to create a graphical user interface of proposed technique. Text file is used for sensitive or high value data to convert it in ciphered form, and then hide it into an image. Both colored and gray scale images are used for steganography. The valuable data has secured in two phases.

In the 1st phase plain text or sensitive data is converted into ciphered text by using RC4 algorithm in which key of 8-2048 bit has been used.

In the 2nd phase that ciphered text is hided into a cover image through using steganography technique of five modulus method. The resulting stego images are computed for varying text file size and after that their level of degradation of that stego images has tested through PSNR.

The sender prospect is shown in Fig. 3.

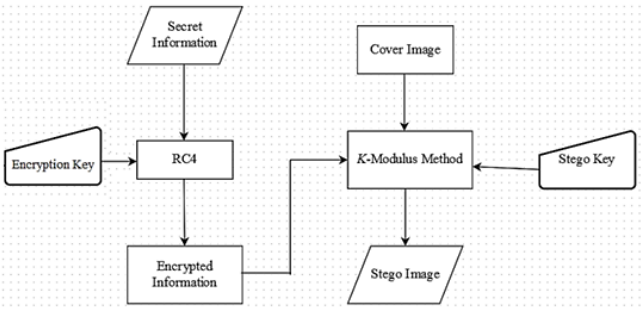


Fig. 3: Sender Prospect

Similarly the receiver prospect is shown in Fig. 4.

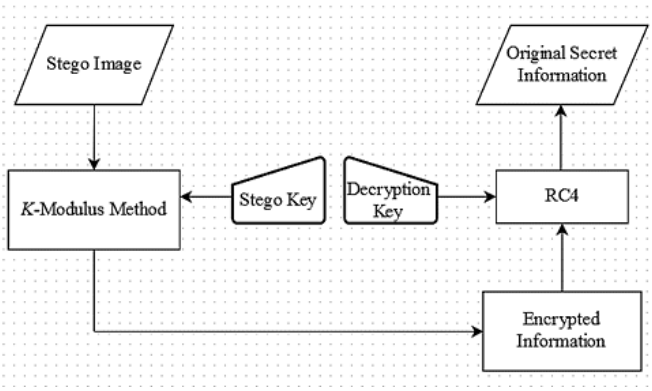


Fig. 4: Receiver Prospect

The main reason behind using these two techniques together is to provide a two layer of security instead of one.

Proposed Solution = Encryption (RC4) + Steganography (k-modulus)

The main advantage of two layer security will be that attackers have to need double time to brake both encryption and steganography only in case of security breach in both layers they will be able to get useful information so probability of their success in one half as compared in case of only one layer security.

A. Working Principle of RC4

The RC4 process creates a pseudo-irregular key stream that is then used to produce the cipher content (by XORing it with the plaintext). It's so called pseudo as it creates a progression of numbers that just approximates the belongings of irregular numbers [17]. The key stream is produced from a variable length key utilizing an inward state made out of the accompanying components:

- A 256 bytes array usually represented as (S) comprising a permutation of these 256 bytes
- Two catalogs s(m) and s(k), used to point elements in the S array (for each index only 8 bits are necessary since the array only have 256 elements).

a) Pseudo-code for key-scheduling algorithm:

for m from 0 to 255
s[m] := m
endfor
k :=0
for m from 0 to 255
k := (k + s[m] + key[m mod key length]) mod 256
swap values of s[m] and s[k]
endfor

This newly created S array will be used in the succeeding step of the RC4 algorithm to create the key stream.

b) Pseudo Code for Pseudo random generation algorithm:

m:=0
k:=0
while generating output:
m := (m + 1) mod 256
k := (k + s[m]) mod 256
swap values of s[m] and s[k]
P := s(s[m] + s[k]) mod 256)
output P
endwhile

After the key stream has been produced, the ciphering of the plaintext is certainly easy: it basically involves a XOR amongst the simple text and the key stream. A sketch of the encryption is shown in Fig. 5.

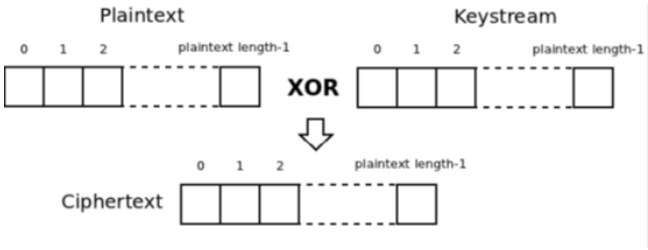


Fig. 5: Sketch of XOR Encoding

For the decoding phase, it is as same as for the encoding; we only have to do the reverse: XOR the cipher text with the key stream as shown in Fig. 6.

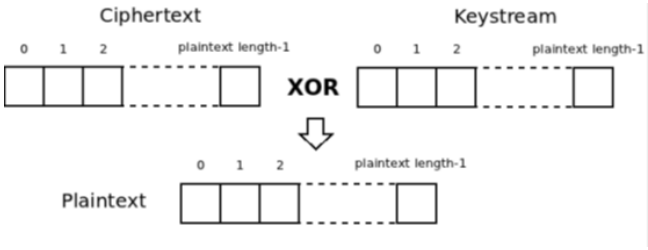


Fig. 6: Sketch for XOR Decoding

B. Working Principle of Five Modulus Method (FMM)

The rudimentary indication behind FMM is the subsequent theory: A conjoint feature in most of the images is that adjacent pixels are associated. Thus, for bi-level images, the neighbors of the pixels are likely to the original pixel. Therefore, FMM comprises distributing the image into parts of K × K pixels apiece. Clearly, in two levels of gray images each pixel has a value between 0 and 255 [18]. Hence, if we can turn every number in this area in a number dividable by five, then this will not affect the human visual system (HVS). The rudimentary idea in the FMM is to rheostat all the pixels in the block K × K and converts each pixel to an integer dividable by 5 according to the following algorithm.

if pixel mod 5 = 4
pixel = pixel+1
else if pixel mod 5 = 3
pixel = pixel+2
else if pixel mod 5 = 2
pixel = pixel-2
else if pixel mod 5 = 1
pixel = pixel - 1

Each pixel value in K×K block is a digital depiction of an image. According to FMM table 1, the conversion of the FMM could be revealed.

TABLE I. FMM TRANSFORMATION

Old Value	New Value	Old Value	New Value
0	0	111	110
1	0	112	110
2	0	113	115
3	5	114	115
4	5	…	…
5	5	221	220
6	5	222	220
7	5	…	…
8	10	253	255
9	10	254	255
10	10	255	255

Here, FMM could convert any integer in the range 0 to 255 in a series so that when we divide it by 5, the reminder is always came 0, 1, 2, 3, or 4, (for example, 23 mod 5 is 3, 14 mod 5 is 4, 200 mod 5 is 0, 182 mod 5 is 2 etc.). Technically, the fresh values for K × K block will always be multiple of 5 as follows: 0,5,10,…,20,25,30,..., 200, 205,210, ..., 250 , 255.

Secondly, as we know that the standard ASCII code comprises of 128 typescripts. But the most common 95 symbols along with characters which are used in binary coding could be mined from the universal ASCII code and represented in table 2.

TABLE II. THE MOST 95 COMMON ASCII CHARACTERS

Dec	Char	Dec	Char	Dec	Char	Dec	Char	Dec	Char
32	space	52	4	72	H	92	\	112	p
33	!	53	5	73	I	93	]	113	q
34	"	54	6	74	J	94	^	114	r
35	#	55	7	75	K	95	_	115	s
36	$	56	8	76	L	96	`	116	t
37	%	57	9	77	M	97	a	117	u
38	&	58	:	78	N	98	b	118	v
39	'	59	;	79	O	99	c	119	w
40	(	60	<	80	P	100	d	120	x
41	)	61	=	81	Q	101	e	121	y
42	*	62	>	82	R	102	f	122	z
43	+	63	?	83	S	103	g	123	{
44	,	64	@	84	T	104	h	124	|
45	-	65	A	85	U	105	i	125	}
46	.	66	B	86	V	106	j	126	~
47	/	67	C	87	W	107	k		
48	0	68	D	88	X	108	l		
49	1	69	E	89	Y	109	m		
50	2	70	F	90	Z	110	n		
51	3	71	G	91	[	111	o		

a) Determination of Window Size

The determination of the appropriate window size is very significant process. The smaller window size is better to surge number of secret message characters hidden in the cover image. A common formula to conclude the appropriate window size has been derived as follows:

$$Window\,\text{size} = \left\lceil \sqrt{\left\lceil \frac{n}{4} \right\rceil} \right\rceil \quad (1)$$

Where 'n' denotes the number of distinctive characters used in the furtive message text. The operator used as a ceiling function to estimate the floating number into the adjacent upper integer and the value of "n = 95" in our case. The number of values inside the K × K window is K^2.

$$Number\ of\ Values\ within\ one\ window = 4K^2 \quad (2)$$

According to above formula this will lodge 4×52=100 value within the 5×5 window size. The general procedure to extract the hidden character ASCII value from that stego or cover image has been derived as follows:

$$Character\ Value = (P + (R-1) \times K^2) + (Si - 1) \quad (3)$$

Where "P" denotes position, "R" denotes Reminder and "Si" denotes starting index. Now, as an descriptive model using 5×5 window size to hide a undisclosed

message sentence “A Steganography Algorithm for Hiding Text in Image Using Five Modulus Method." in the concealment image, the pixel result is shown in table 3.

TABLE III. STEGO IMAGE PIXELS

35	70	60	65	65	61	50	55	55	60
50	115	110	110	110	120	105	105	110	110
35	115	120	110	110	125	115	105	110	110
35	117	115	110	105	115	105	100	105	105
50	120	120	120	115	115	110	120	115	115

65	70	75	80	80	80	90	85	85	85
113	110	110	110	105	105	105	100	100	105
110	110	110	110	105	105	110	110	110	110
105	110	110	110	110	105	115	110	105	105
115	115	115	110	110	105	124	115	110	110

Clearly in the first 5×5 window size all integer inside are modulus of 5 except 117 and 117 mod 5 remainder came 2 which means two loops. Similarly the location of 117 in the first window is 9 by column-wise locating. So according to method, the value of the hidden character is computed as: (9 + (2-1)*52) + 31 = 65 and if we see its value in table 2, it is ASCII code for A. The value of 25 was used as the square of the window size, 52=25. Likewise, since the starting decimal character of the 95 most recurrent ASCII characters is 32, to make the numbering starting from 1, the number of 31 was used. An analogous method may be applied to the rest windows as follows. Therefore, for 61= (1+ (1-1)*25) + 31 =32 which is ASCII code for space. Also, 113 = (2 + (3-1)*25) + 31 = 83 which is ASCII code for S. Finally, 124= (10+ (4-1)*25) + 31 = 116 which is ASCII code for t.

IV. RESULTS & DISCUSSION

The graphical user interface (GUI) in Mat Lab of the proposed techniques for both RC4 encryption and FMM steganography algorithms are shown below in Fig. 7.

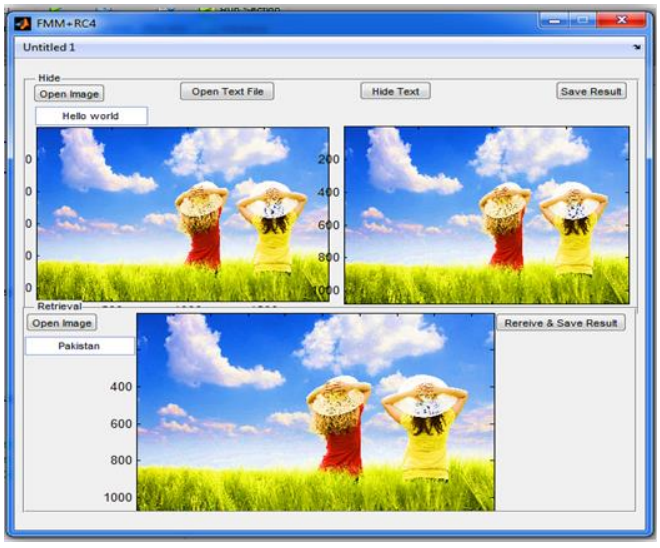
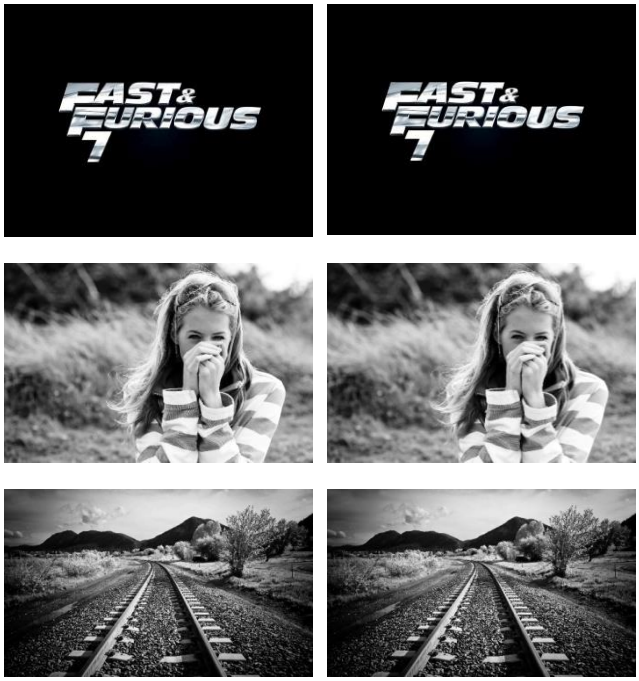


Fig. 7: GUI for both RC4 and FMM

Technique is tested over different images of different size both of colored and gray scale from which few has been shown in Fig. 8 and Fig. 9 respectively.

Fig. 8: Original colored images (left) with their stego Images (right)



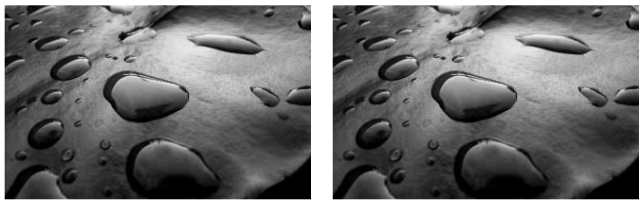


Fig. 9: Orignal Gray scale images (left) with their stego images (right)

From above both colored and gray scale figures result, we can see that the human eye can't discriminate between the original images and the renovated stego images of FMM transformed. The stego image quality can be checked through PSNR (dB) value, higher the value the enhanced is the eminence of recreated image. The PSNR (dB) was calculated for all the test images. The result has been listed for colored images in table 4.

TABLE IV. PSNR (DB) OF COLORED STEGO IMAGES

Image	PSNR
Chicks	45.28
Girl	45.15
Pepper	46.85
Boy	45.13
Flower	45.16

For gray scale images the PSNR (dB) is shown in table 5.

TABLE V. PSNR (DB) OF GRAY SCALE STEGO IMAGES

Image	PSNR
Fast & Furious 7	53.34
Girl	45.17
Railway track	45.25
Water drops	45.30

The results of proposed technique for colored and gray scale images after hiding the text file of different size is shown below in table 6 for colored images and in table 7 for gray scale images.

TABLE VI. PSNR (DB) FOR TEST IMAGES (COLORED)

Text File Size	Girl	Boy	Peppers
1 KB	45.158	45.135	46.852
2 KB	45.106	45.116	46.833
4 KB	45.102	44.987	46.821
6 KB	45.1	44.914	46.803
8 KB	44.984	44.874	46.786
10 KB	44.982	44.856	46.771
12 KB	44.898	44.793	46.756

TABLE VII. PSNR (DB) FOR TEST IMAGES (GRAY SCALE)

Text File Size	Fast & Furious	Railway Track	Water Drops
1 KB	53.343	45.252	45.302
2 KB	53.340	45.163	45.289
4 KB	53.331	45.081	45.187
6 KB	53.329	44.934	45.106
8 KB	53.317	44.901	45.007
10 KB	53.287	44.804	44.983
12 KB	53.251	44.787	44.977

In the both tables 6 & 7, the PSNR values clearly showing that this is an efficient technique which hides the encrypted text in an image without noticeable distortion in cover image. This ratio or proportion is frequently utilized as quality estimation between the first and a compacted picture. By examining the result listed above in tables we can say that the prosed integrated technique is efficient and better as compared to many more which have more complexity and lack satisfactory result. Secondly simple GUI for this technique makes it easy to use as compared to many others in which two different interfaces makes them irritating for human interaction.

V. CONCLUSION AND FUTURE WORK

A novel technique comprising steganography along with cryptography based on the RC4 and FMM method has been proposed. Many researchers have been reported different techniques but all the methods suffer with image quality problem or image size or format restriction. While in our proposed novel technique there is no such limitation of image size or format or even either it's colored or gray scale. Thus this novel technique can efficiently be implemented over an image of any format or size. While data security and safety point of view and to achieve good quality along with security, the implementation of the FMM along with RC4 produces better results and easily can carry the encrypted information and sent to the destination without being visible by hackers or HVS. The stego

images were also verified using PSNR value even when we increased the size of text file from 1KB to 10 KB then also to an unbelievable extent a very little decrease in PSNR value occurs. So according to the PSNR test results, the stego images carrying encrypted data have high PSNR. Hence, the proposed novel technique is an efficient technique to hide the encrypted text inside an image without having noticeable distortion.

For future work there are some issues that need to be resolved. One of these issues is that the 5×5 window size is large to accommodate one secret letter. According to formula when using all of the 256 ASCII characters an 8×8 window size will be used. So this window size is large and will affect the image quality which needs to be improved by some methods. Also in future the security features of the steganography and cryptography can highly be optimized by using genetic algorithm. So in future combined both visual cryptography and FMM can be improved with Genetic Algorithm.

REFERENCES

[1] B. Schneier, “Security in the Real World: How to Evaluate Security Technology”, Computer Security Journal, vol. 15, pp.1-14, June 1999.

[2] A.B. Ibrahim A.A. Kadi, "The origins of cryptology: The Arab contributions”, Cryptologia, vol. 16, pp.97–126, April 1992.

[3] A. Singh, A. Nandal and M. Swati, “Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security", International Journal of Advanced Research in computer Science and Software Engineering, vol.2, pp. 39-49, December 2012.

[4] S.B Sasi, D. Dixon, J. Wilson, “A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security”, IOSR Journal of Engineering (IOSRJEN), vol. 04, pp. 01-04, March 2014.

[5] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt, “Digital Image Steganography: survey and analyses of current methods”, signal processing, vol. 90, pp.727-752, March 2010.

[6] W. Stallings, Principles and practices, 5th ed. “Cryptography and Network Security". Pearson education, pp.28-34, 2003.

[7] Menezes, Alfred, C. Paul, V. Oorschot, S. Vanstone, 5th ed. “Handbook of Applied Cryptography” CRC Press, August 2001, pp.2-49.

[8] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy Mag., vol. 1, pp. 32–44, March 2003.

[9] B. Svet, “Secure Sockets Level, Steganography” [ONLINE] Available at: ww.cs.buffalo.edu/~sbraynov/lectures/lecture6_pdf . [Last Accessed 20 March 2015].

[10] S. Suri, H. Joshi, V. Mincoha and A. Tyagi, "Comparative Analysis of Steganography for Coloured Images", International Journal of Computer Sciences and Engineering, vol.2, pp.180-184, April 2014.

[11] M.K. Sharma, A. Upadhyaya and S. Agarwal, "Adaptive Steganographic Algorithm using Cryptographic Encryption RSA Algorithms", Journal of Engineering, Computers & Applied Sciences (JEC& AS), vol.2, January 2013.

[12] M.I. Hussain and M.D. Hussain, “A Survey of Image Steganography Techniques” International Journal of Advanced Science and Technology Vol. 54, pp.113-123, May, 2013.

[13] E. Walia, P. Jain, and C. Navdeep, “An Analysis of LSB & DCT based Steganography”, Global Journal of Computer Science and Technology, vol. 10, pp. 4-8, April 2010.

[14] G.V. Manoj, T. Senthur, M. Sivasankaran and M. Vikram, "AES BASED STEGANOGRAPHY", International Journal of Application or Innovation in Engineering & Management, vol.2, pp.382-389, January 2013.

[15] R. Joshi, L. Gagnani, S. Pandey, “Image Steganography With LSB” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, pp. 228-229, January 2013.

[16] N.H. Nazmudeen and F.J. Farsana, "A New Method for Satellite Image Security Using DWT-DCT Watermarking and AES Encryption" International Journal of Innovative Research in Science, Engineering and Technology, vol.3, pp. 69-76, July 2014.

[17] L.M. Nannaka, H. Singarapu and P. Ramadevi, "Remodelling RC4 Algorithm for Secure Communication for WEP/WLAN Protocol", Global Journal of researches in engineering Electrical and electronics engineering , vol.12, online ISSN:2249-4596, April 2012.

[18] F.A. Jassim and H.E. Qassim, "Five Modulus Method For Image Compression", Signal & Image Processing : An International Journal (SIPIJ), vol.3, pp.19-28, October,2012.