LZW DATA COMPRESSION FOR FSP ALGORITHM

Dr. C. Parthasarathy [1], G. Kalpana [2], V. Gnanachandran[3]

[1]Assistant Professor, Dept. of IT SCSVMV University, Enathur, Kanchipuram Pin – 631 561
[2]Assistant Professor, SCSVMV University Enathur, Kanchipuram Pin – 631 561
[3]Assistant Professor, Pattammal Alagesan Arts and Science College, Athur, Chengalpet
sarathy286089@rediffmail.com kalpana_mscit@yahoo.co.in
gnanamchandran@yahoo.com

ABSTRACT

The main objective of this paper is to detect the existence of secret information hidden within an image. Cryptography is one of the most interesting and important area in the computer industry that deals with secure transmission of information. Encryption, the process which helps for such secure transmission, prevents hackers from accessing the information. Decryption helps to retrieve the original information. Cryptography provides many methods and techniques for secure communication. The new scheme is designed to be backward-compatible, that is, a file compressed with our error-resilient algorithm can be still decompressed by the original decoder. In this paper, we deal with the popular Lempel-Ziv-Welch compression scheme. The algorithm manipulates a 128-bit input using flipping, substitution, and permutation to achieve its encryption/decryption.

KEYWORDS

Compression, Cryptography, Flipping, Permutation, Folding.

1. INTRODUCTION

This FSP simple encryption/decryption algorithm that is fast and fairly secure. The algorithm manipulates a 128-bit input using flipping, substitution, and permutation to achieve its encryption/decryption. The secret data will be flipping, substitute and permutation and stored in the protected image. The client computer sends the information with the help of eight different processes. A low-complexity grayscale image embedding scheme that can embed multiple secret images is proposed in this paper. In this scheme, different users can extract different secret images according to the secret keys they hold. To reduce the storage cost of the secret images, each of the secret images is first compressed using an improved version of the moment preserving block truncation coding scheme. The compressed message of each secret image is then encrypted by the FSP cryptography system with different secret key and then embedded into the host image using the modulus least-significant-bit substitution technique. LZW is a lossless data compression algorithm developed by T. Welch in 1984 for implementation in hardware for high-performance disk controllers.

DOI : 10.5121/ijait.2012.2503

2. DESIGN ISSUES

1. Restrict the key size: An algorithm's key length is distinct from its cryptographic security, which is a logarithmic measure of the fastest known computational attack on the algorithm, also measured in bits. The security of an algorithm cannot exceed its key length but it can be smaller. For example, Triple DES has a key size of 168 bits but provides at most 112 bits of security.FSP algorithm comes the closest with an effective security of its key length.
2. Encrypt with large files: Encryption is done with smaller files for secured transmission by keeping the memory consumption less.
3. Scalability and concurrency: The algorithm used to generally scalable and also concurrency is achieved among the four users Author module, CS module. Buyer module, Control authority module.
4. Confidentiality: The encrypted algorithms can verify confidentiality while sending and receiving the secret data.
5. Authentication: The authentication is accepting proof of identity given by a credible person, which has evidence on the said identity or on the originator and the object under assessment as his artifact respectively.
6. Suitable for wide range of application: The innovation opens the door to a wide range of applications.
7. Analysis to find the efficiency of keys: Brute force attack technique ensures the key strength.

3. PROPOSED ALGORITHM

Secure communication with the help of FSP algorithm is as follows:

Step 1: The flipping bit is set.
Step 2: The characters are changed according to the flipping bit.
Step 3: The ASCII table is checked and the keys found out.
Step 4: With the help of the keys, square matrix is made, using inverse table.
Step 5: Flipping operation is done.
Step 6: The steps 2 to 5 are repeated.

4. FLIPPING OPERATION

One piece of the secret information is the flipping key and its length is 128 bits, and it is used to obscure the plaintext or cipher text further, Given a 128-bit input PT (Plain Text) and a flipping key F, we denote the flipping operation on PT as follows:

Output=Flip (F, PT)

In the flipping operation, 128- bit input is disguised as follows: For each bit of the input, if the corresponding bit of the flipping key is 1, the corresponding output bit will be the complement of the input bit. That is, if the flipping key bit is 0 and the input bit is 0/1, the output of the flipping operation is 0/1. On the other hand, if the flipping key bit is 1 and the input bit is 0/1, the output of the flipping operation is 1/0. In reconstructing the original input, the output of the flipping operation is flipped against the same flipping key.

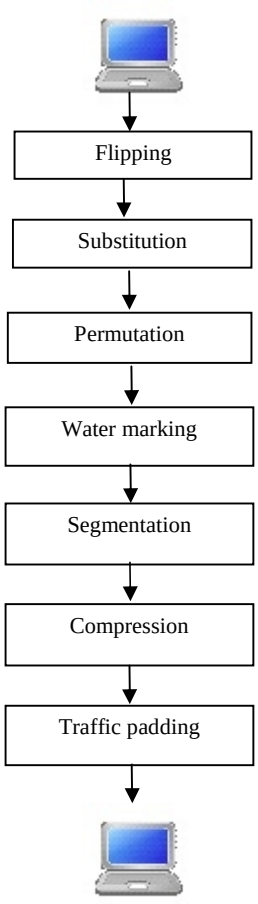

Figure 1. Client side processing

5. SUBSTITUTION OPERATION

The substitution operation uses the following five tables:

1. ASCII Table
2. Subset Table
3. Block Table
4. Substitution Table
5. Inverse Substitution Table

Our algorithm uses substitution and inverse substitution table for encryption and decryption .These tables are generated based upon the ASCII code and the key. Let PT be the plain text, CT be the cipher text and key be the flipping key. In this, plain text is text file. This file will have all the ASCII characters. The ASCII characters are given in Table In this, the rows indicate the left digit and the column indicates the right digit. Again this table is subdivided into subsets. For dividing the subset into blocks, we have to follow the following procedure. If the number of characters is less than or equal to 10, we have to divide this into two halves. If the number of characters is even number, we divide it into equal halves. Suppose, the number of characters is odd number, we have to divide this into 2 subsets but the size of the first subset is greater than the

second subset by 1. To construct the substitution table 2, key is used and it will be informed to the receiver in a secure manner. Suppose the key K is given by

K= 6 7 10 3 5 12 4 8 1 13 9 2 14 11 15

[Numbers 1 to 15 occur once & only once in the key and correspond to Table 1]

Table 1 . ASCII Table.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
3			Blank	!	“	#	$	%	&	‘
4	(	)	*	+	,	-	.	/	0	1
5	2	3	4	5	6	7	8	9	:	;
6	<	=	>	?	@	A	B	C	D	E
7	F	G	H	I	J	K	L	M	N	O
8	P	Q	R	S	T	U	V	W	X	Y
9	Z	[	\	]	^	_	`	a	b	C
10	D	E	F	G	h	i	j	k	l	M
11	N	O	P	Q	r	s	t	u	v	W
12	X	Y	Z	{	|	}	~			

The key K starting value 6 stands for the 6th block in the block table that has the following 7 characters A B C D E F G whose ASCII values are 65,66,67,68,69,70 and 71 respectively. We fill up the initial four values 0, 1, 2, 3, 4, 5, 6 and 7 for substitution table in those positions. Table 2 shows the substitution values.

The second key k value is 7. We go over to 7th block that contains H I J K L M whose ASCII values range from 72 to77. Hence, in substitution table, they are given 4, 5, 6, 7, 8 and 9. Following the same procedure, all other ASCII values are given their corresponding substitution values. The inverse happens in case of inverse substitution table where we put 65 for 0, 66 for 1, 67 for 2, 68 for 3 and so on. Table 3 shows the inverse operation.

Table 2. Substitution Table.

	0	1	2	3	4	5	6	7	8	9
3			49	50	51	52	53	54	55	56
4	70	71	72	73	74	75	76	77	19	20
5	21	22	23	37	38	39	40	41	24	25
6	26	27	28	29	30	0	1	2	3	4
7	5	6	7	8	9	10	11	12	42	43
8	44	45	46	47	48	64	65	66	67	68
9	69	13	14	15	16	17	18	84	85	86
10	87	88	89	90	31	32	33	34	35	36
11	57	58	59	60	61	62	63	78	79	80
12	81	82	83	91	92	93	94			

Table 3. Inverse Substitution Table.

	0	1	2	3	4	5	6	7	8	9
0	65	66	67	68	69	70	71	72	73	74
1	75	76	77	91	92	93	94	95	96	48
2	49	50	51	52	58	59	60	61	62	63
3	64	104	105	106	107	108	109	53	54	55
4	56	57	78	79	80	81	82	83	84	32
5	33	34	35	36	37	38	39	110	111	112
6	113	114	115	116	85	86	87	88	89	90
7	40	41	42	43	44	45	46	47	117	118
8	119	120	121	122	97	98	99	100	101	102
9	103	123	124	125	126					

6. PROPOSED FOLDING TECHNIQUE FOR PERMUTATION OPERATION

The origin of folding is from paper folding. This folding is broadly divided into three types:

1. Vertical folding
2. Horizontal folding
3. Diagonal folding

Figure 2 shows vertical folding technique.

PLAIN TEXT				
A	F	**K**	P	U
B	G	**L**	Q	V
C	H	**M**	R	W
D	I	**N**	S	X
E	J	**O**	T	Y

Figure 3 shows horizontal folding technique.

CIPHER TEXT				
U	P	**K**	F	A
V	Q	**L**	G	B
W	R	**M**	H	C
X	S	**N**	I	D
Y	T	**O**	J	E

Figure 2 .Vertical folding technique

Suppose there are 5 rows present in the plain text document. Cipher text is created with respect to following folding technique:

1 ↔ 5
2 ↔ 4
3 ↔'3

In the case of vertical folding method, columns are exchanged dynamically. It is same as horizontal folding using column processing instead of row processing.

PLAIN TEXT				
A	B	C	D	E
F	G	H	I	J
K	**L**	**M**	**N**	**O**
P	Q	R	S	T
U	V	W	X	Y

CIPHER TEXT				
U	V	W	X	Y
P	Q	R	S	T
K	**L**	**M**	**N**	**O**
F	G	H	I	J
A	B	C	D	E

Figure 3. Horizontal folding technique

The diagonal folding method must be implemented in square matrix arguments. If not, proper padding must be added to get the appropriate solution. On the side of decryption, padding must be eliminated after processing.

7. ENCRYPTION LEVEL

The last piece of the secret information is the encryption level. It is a positive integer. The higher the encryption level is, the more secure the algorithm is. However, we should be cautious with large values of the encryption level since an increase of the encryption level is proportional to the decrease of the encryption / decryption speed.

8. SEGMENTATION

Picture segmentation refers to the process of partitioning a digital image into multiple segments. The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to locate objects and boundaries in images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain visual characteristics.

9. COMPRESSION

Lossless compression decreases the size of an image without compromising the information contained in an image. In view of this characteristic, data that has been compressed using lossless algorithms can be restored back into to its original form without any artifacts. Common applications for lossless compression techniques include facsimile encoding for transmission and progressive image transmission. Image compression makes the job of an intruder more difficult. The objective to implement an efficient adaptive compression algorithm error resilient LZW.

Lossless data compression systems are typically regarded as very brittle to transmission errors. This limits their applicability to domains like noisy tether less channels or file systems that can possibly get corrupted. Here we show how a popular lossless data compression scheme used in file formats GIF, PDF, and TIFF, among others, can be made error-resilient in such a way that the compression performance is minimally affected.

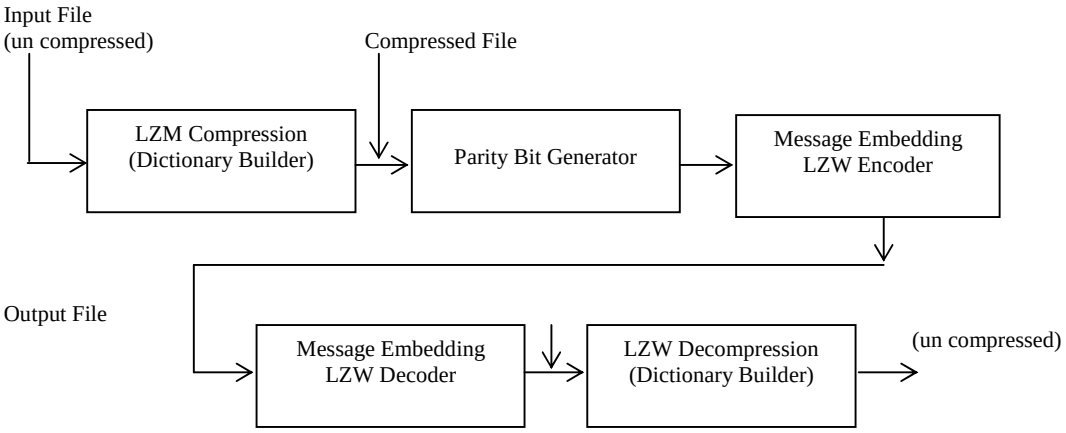

Figure 4. System block diagram

10. TRAFFIC PADDING

Effective countermeasure to traffic analysis is traffic padding. Traffic padding is one of the functions of link encryption approach. It produces cipher text output continuously in the picture; even in the absence of plaintext, a continuous random data stream is generated.. When input plaintext is not present, random data are encrypted and transmitted.

10.1. Advantages of traffic padding

It is impossible for an attacker to distinguish between true dataflow and padding data flow.

- It is impossible to deduce amount of traffic.
- It is difficult to identify the critical nodes

ALGORITHM:

Step 1: The required class for Java is imported.
Step 2: The required values are initialized to the appropriate parameters.
Step 3: The length of the values is checked.
Step 4: The length is declared using a for loop.
Step 5: For adding an extra bit, the length should be less than 5.
Step 6: The output is obtained.
Step 7: Stop

11. BRUTE FORCE ATTACK

To hack into the FSP encryption/decryption algorithms using the brute force approach, one needs to guess the flipping key, the substitution function, the permutation function and the encryption level. A brute force attack, an exhaustive key search, is a strategy that can in theory be used against any encrypted data by an attacker who is unable to take advantage of any weakness in an encryption system that would otherwise make task easier. It involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space. The resources required for a brute force attack scale exponentially with increasing key size. As a result, doubling the key size for an algorithm does not simply double the required number of operations, but rather squares them. There are 128 bits in a key. Each bit can be either 1 or 0. Therefore, there are 2128 flipping keys.

12. CONNECTION METHOD

Computer networks can be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as optical fiber, Ethernet, Wireless LAN, Home PNA, power line communication or G.hn.. Ethernet, as it is defined by IEEE 802, utilizes various standards and media that enable communication between devices. Frequently deployed devices include hubs, switches, bridges, or routers. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium. ITU-T G.hm technology uses existing coaxial cable, phone lines and power lines to create a high-speed (up to 1 Gigabit/s) local area network.
Server side algorithm:

Step 1: Start.
Step 2: The image file is selected.
Step 3: The information is encoded into the image file.
Step 4: The image is passed on image splitter application. The number of segments is entered as input.
Multiple image files will be created.
Step 5: Using socket programming, a connection is established between client and server.
Step 6: Different segments are passed as file objects to the server after connecting to the server.
Step 7: Stop.

Initially the secret data is converted into cyber text from plain text. Under flipping process, the secret data is converted into binary form and its complement is substituted using ASCII table. Under substitution process, with the help of subset table, block table, substitution table and inverse substitution table, the processed data attains full encryption. To give a full protection, fully encryption data is randomly mixed. The mixed process was done by three crucial techniques, vertical folding, horizontal folding, and diagonal folding. The above said FSP process is done for 9 levels with different combinations of the FSP technique. The output of the above

process is embedded over a picture. The present file is now split into five segments. Each segment is now compressed by lossy algorithm. After the above compression, each binary output is added with four extra bits, either in left or right randomly, by traffic padding technique. After the above regress encryption exercises, the file is sent to the receiver. The receiver of the file then decrypts the file to get the original secret data. This done as follows:

1. Reverse traffic padding
2. Decompression
3. Stick together.

After the clipping process, the image is retrieved.By the help of image processing technique, the secret data which was encrypted is fully retrieved. Again, by reverse FSP technique, the original data is fully got.

13. STEGANALYSIS

Steganalysis has recently attracted researcher's interests with the development of information hiding techniques.A particular watermarking or hidden data scheme leaves statistical evidence or structure that can be exploited for detection with the aid of proper selection of image features and multivariate regression analysis. We use some sophisticated image quality metrics as the feature set to distinguish between watermarked and unwatermarked images. To identify specific quality measures, which provide the best discriminative power, we use analysis of variance (ANOVA) techniques. The multivariate regression analysis is used on the selected quality metrics to build an optimal classifier using images and their blurred versions. The idea behind blurring is that the distance between an unwatermarked image and its blurred version is less than the distance between a watermarked image and its blurred version. Simulation results with a specific feature set and a well-known and commercially available watermarking technique indicate that this approach is able to accurately distinguish between watermarked and unwatermarked images.

14. FUNCTIONAL POINT ANALYSIS

Function Point Analysis has been a reliable method for measuring the size of computer software. In addition to measuring output, Function Point Analysis is extremely useful in estimating four module in ECMS.

15. DESIGN AND TEST PLAN

The System Design Document (SDD) shows how the proposed system will be structured to satisfy the requirements identified in the software requirements specification. This describes how the requirements are translated into software structure, components, interfaces and data.

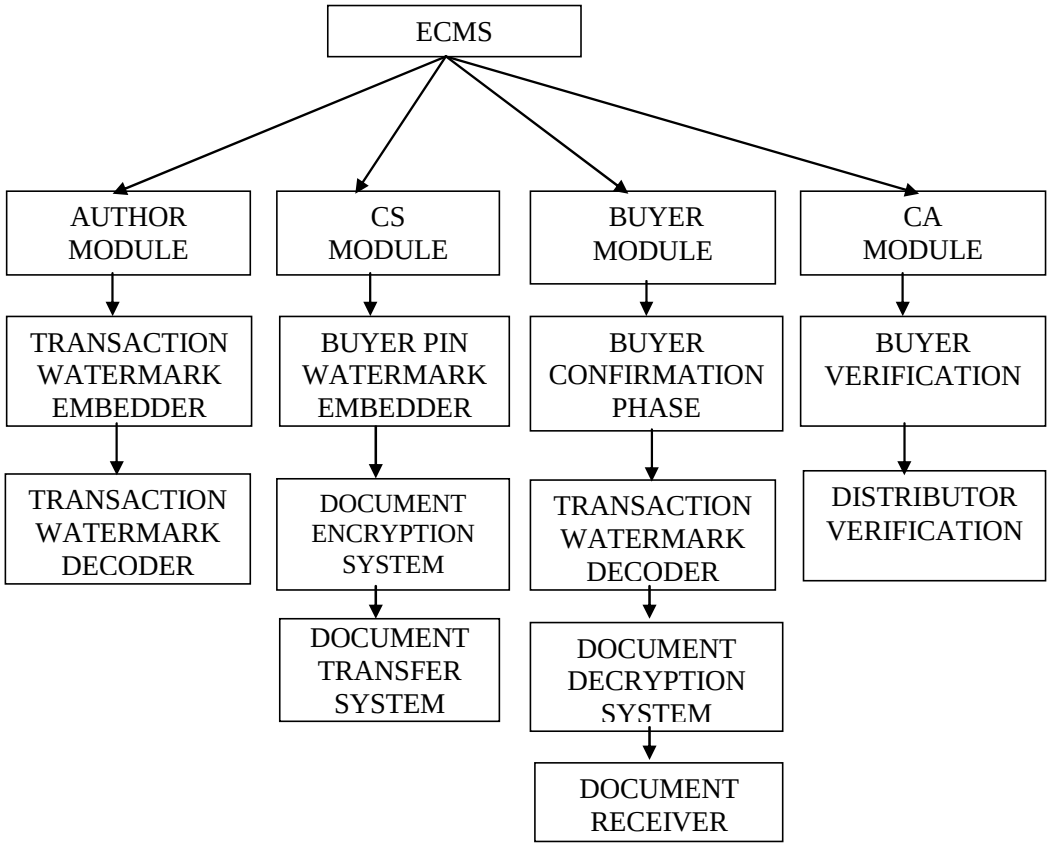

Figure 5. Electronic copyright management system module

16. CONCLUSION

This paper addresses the problem of copyright protection in open network environments. Author module embeds the CUN and distributor PIN in the image. In this module, FSP algorithm is used to generate public and private keys. CS module embeds the Buyer's PIN into the image using CS private key. Hash value of the image is computed using hashing algorithm. It helps for authentication purpose. In buyer module, hash value of the received image is computed using hash function. Buyer confirmation phase is used for authentication purpose.CA module detects illegal usage.

The software used needs facility of monitoring and analyzing intruders and raising an alarm with a new technique. The FSP encryption/ decryption algorithm is a simple algorithm based on the flipping, substitution and permutation operations. It is fast and fairly secure. However, it is only suitable for applications that do not expose the inputs and the encrypted form of the inputs to the public. If there is a need for the applications to expose its inputs and its encrypted forms of the inputs, then it should use the FSP encryption/decryption algorithm instead. Link encryption can also, protect against forgery if used properly in ECMS system. It is a simple concept that can fit transparently into existing communication applications.

ACKNOWLEDGMENTS

Our thanks to Sri Chandrashekarendra Saraswathi Viswa Mahavidyalaya University for providing possessions to carry out this project.

REFERENCES

[1] Whitfield Diffie and Artine E.Hellman (2010), "New directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp. 85-94.

[2] J. Fridrich, M. Goljan and R. Du (2001), "Reliable Detection of LSB Steganography in Color and Gray-Scale Images", Magazine of IEEE Multimedia Special Issue on Security, pp. 22-28.

[3] N. Jacobsen, K. Solanki, U. Madhow, B. S. Manjunath and S. Chandrasekaran (2002), "Image-adaptive high-volume data hiding based on scalar quantization", Proc. IEEE Military Communications Conference (MILCOM), Anaheim, CA, USA, Vol. 1, pp.411-415.

[4] A. Westfeld (2003), "High Capacity Despite Better Steganalysis (F5A Steganographic Algorithm)", LNCS Vol.2137, Springer-Verlag, New York, Heidelberg, Berlin, pp. 289-302.

[5] Alessandro Piva, Franco Bartolini, and Mauro Barni (2002), "Copyright protection in Open networks", IEEE Internet Computing, pp. 87-95.

[6] Kalaichelvi. V and RM.Chandrasekaran (2008), "FSP Algorithm for encryption/ decryption", ICCCN 2008, Proceedings of the International conference on computing and communication network, Karur, Tamilnadu, pp.245-251.

[7] Rade Petrovic (2003), "Copyright Protection based on Transaction watermark", IEEE, Vol.2, 0-7803-7963-2, pp.509–518, Telecommunications in Modern Satellite, Cable and Broadcasting Service, San Diego, CA, USA, 10.1109/ TELSKS. 2003.1246278, 8007683,http://ieeexplore.ieee.org/ xpl/freeabs_all.jsp? tp=&arnumber = 1246278&isnumber=2796.

[8] Richard Smith (2002), "Internet Cryptography", Pearson Edn. Pvt. Ltd, 2nd Edition, ISBN 0-201-92480-3, pp. 39- 44, Boston, MA 02131 USA DOI:10.1016/S0172-2190(00)00042-9,http://www.flipkart.com/ internet-cryptography -Richard-e-Smith/0201924803-jqw3fygjfb.

[9] T. Furon, I. Venturini, and P. Duhamel (2001), "Unified Approach of Asymmetric Watermarking Schemes",2002, Security and Watermarking of Multimedia Contents III, P.W.

[10] Wong and E. Delp, eds., Proc. SPIE, Vol. 4314, 2001, pp. 269-279,DOI10.1109/ MIC.2002.1003126,http://www2.computer.org/portal/web/ csdl/doi/ 10.1109/ MIC.2002.1003126.

[11] Tsuhan Chen, Kou-Sou Kan and Ho-Hsun Chang (2003), "Watermarking 2D/3D Graphics for Copyright Protection", IEEE ICASSP 2003, Vol. 4, pp. IV- 720-3, ISBN: 0-7803-7663-3, Internet & Multimedia Lab., Chunghwa Telecom Labs, Taoyuan,Taiwan, 7810434, http://ieeexplore.ieee.org / xpl / freeabs_ all.jsp?arnumber =1202744.

[12] Wei Li, Xiangyung Xue, and Peizhong Lu (2003), "A Novel Feature-based Robust Audio Watermarking for Copyright Protection", IEEE Computers and Communication 2003,ISBN:0-7695-1916-4,554-560,Washington,DC,USA,http://portal.acm.org/ citation.cfm ? id = 845903.

[13] William Stallings (2008), "Cryptography and Network Security", Pearson Edn. Pvt. Ltd, 2008, 4th edtion, ISBN 13:9780132023221,pp. 26-29, Akhil books Pvt Ltd,India,DOI-10.1155/2008/529879,http://www.alibris.co.uk/search/books/ qwork/ 8988407/ used/ Cryptography%20 and%20Network%20Security.

[14] Anderson Petitcolas, Anderson.R and Petitcolas.F (2001), "On the limits of the steganography", IEEE Journal Selected Areas in Communications, No.16, pp. 4474-4481.

[15] Bassia, P., Pitas, I and Nikolaidis, N (2001), "Robust audio watermarking in the time domain", IEEE Transactions on Multimedia, 3, 2, pp.232-241.

[16] Yonghui Wu Lonardi, S. Szpankowski, W. (2006) , Error-resilient LZW data compression, pp. 193 – 202, Proceedings of the Data Compression Conference (DCC;06), IEEE, ISSN : 1068-0314.

AUTHORS

Dr. C.Parthasarathy has been working as a Assistant professor in the Department of Information Technology in Sri Chandrashekhendra Saraswathi Viswa Maha Vidyalaya University, Enathur, Kanchipuram –631561 since 2006. He has completed his M.C.A from in Madras University, and M.Tech in Sathyabama University M.Phil in Computer Science from Annaamalai University and Ph.D Chanrashekhendra Saraswathi Viswa Maha Vidyalaya University, Enathur. Since January 1st 2001 Dr. C.Parthasarathy has been a Lecturer in various colleges. He has been research in Network Security. He is currently focusing on the creating a new algorithm in Steganography.

G. KALPANA has completed his M.SC(IT). Now she is Mphil scholar in SCSVMV UNIVERSITY, Enathur, Kanchipuram. She is currently focusing on the creating a new algorithm in Wireless communication.

V.Gnanachandran has been working as a Assistant professer in the PattammalAlagesan Arts and Science College Ettikuttimedu Village, Maduramangalam Post, Kanchipuram Kanchipuram Dt Pin - 602 108. He has compled his M.Sc from Kanchi Shri Krishna College Of Arts and Science, Kanchipuram, M.Phil from Computer Science in Centre for Distance Education, Bharathidasan University, Tiruchi., B.Ed from Computer Education in IASE , Saidapet and M.A(Edu.)., M.A(Eng.) from Alagappa University (CDE), Karaikudi.