Asian Journal of Information Technology 8 (3): 67-73, 2009
ISSN: 1682-3915
© Medwell Journals, 2009

Electronic Copyright Management System

[1]C. Parthasarathy and [2]S.K. Srivatsa
[1]Department of CSE, Sri Chandrashekhendra Saraswathi Viswa Mahavidyalaya University, Enathur, Kanchipuram 631 561, India
[2]St. Joseph's College of Engineering, Jeppiaar Nagar, Chennai 600 064, India

Abstract: The main objective of this study is to detect the existence of secret information hidden within an image. Cryptography is one of the most interested and important area in the computer industry that deals with secures transmission of information. Encryption, the process, which helps for such secure transmission prevents hackers to access the information. And decryption helps to retrieve the original information. Cryptography provides many methods and techniques for secure communication. Currently, there are many industry standard encryption/decryption algorithms including RSA, AES, Robust Security Network (RSN), blowfish and so forth. However, they are fairly complex and require that one spend a lot of time to comprehend and implement them. This study introduces simple Encryption/decryption algorithm that is high-speed and practically make safe. The algorithm manipulates a 128-bit input using flipping, substitution and permutation to achieve its encryption/decryption.

Key words: Cryptography, hacker, security, steganography, watermarking, encryption, decryption

INTRODUCTION

Steganalysis has recently attracted researcher's interest with the development of information hiding techniques (i.e., Steganography). 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 un watermarked 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 the optimal classifier using images and their blurred Versions (Rade, 2003). The idea behind blurring is that the distance between an un-watermarked 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 indicates that this approach is able to accurately distinguish between watermarked and un watermarked images.

Recently, Computer technology has been highly developed. Numerous applications of various types have been written. Many of them require that their data be secured from unwelcome users. Different types of applications require specialized security levels. Security is the primary concern of all those people who deal with activities, which involve protection of risk. The branch of science cryptography, which is concerned with the security of information, developed in the hands of military people and it was nurtured by them for quit long time as their private property. For this reason, many algorithms are developed for encryption and decryption, which provides high security. All these algorithms are kept open to the public and the secrecy of the algorithm lies entirely in the key. This study stands different that the development of algorithm addresses the user needs in specific, thereby offering more flexibility. We show that visible watermarks can be added to 2D data and detected reliably. The watermarks can be designed to be robust to quantization of the vector data and several other hostile attacks (Tsuhan *et al*., 2003).

MATERIALS AND METHODS

The whole point of cryptography is to keep the plaintext (or the key or both) secret from eavesdroppers (also called adversaries, attackers, interceptors, interlopers, intruders, opponents or simply the enemy).

Corresponding Author: C. Parthasarathy, Department of CSE, Sri Chandrashekhendra Saraswathi Viswa Mahavidyalaya University, Enathur, Kanchipuram 631 561, India

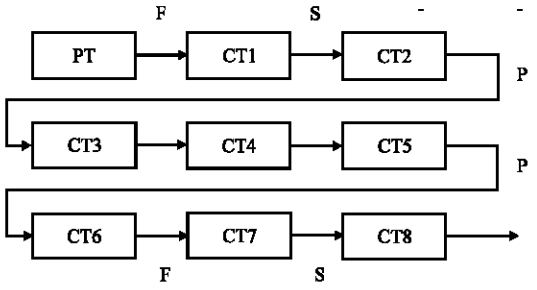

Fig. 1: Encryption with 8 levels

Eavesdroppers are assumed to have complete access to the communication between sender and receiver (Bruce, 2001). Here, we describe the Finite State Projection (FSP) algorithm used to encrypt and decrypt secret information embedded in an image.

Figure 1 shows PT is the Plain text and CT is the Cipher text. The encryption is done in 8 levels using F flipping key and substitution (s) and permutation (p) operations to get the final CT.

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:

$$\text{Output} = \text{Flip}(F, PT)$$

In the flipping operation, its 128-bit input is disguised as follows: For each bit of the input, if the corresponding bit of the flipping key is 0, 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.

Substitution operation: This 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 as a text file. This file will have all the ASCII characters. The ASCII characters are given in the Table 1. In this, the rows indicate the left digit and the column indicates the right digit.

Again this table is subdivided into subsets as given in Table 2 (Subset Table). For dividing the subset into

Table 1: ASCII table

Digits	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	{	|	}	~			

Table 2: Subset table

Type	Code	No. of characters
Special characters	32-47	16
Digits	48-57	10
Special characters	58-64	7
Uppercase letters	65-90	26
Special characters	91-96	6
Lowercase letters	97-122	26
Special characters	123-126	4

blocks as given in Table 3 (Block Table), we have to follow the following procedure. If the no 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 4, it uses key and it will be informed to the receiver in a secure manner.

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

Numbers 1-15 occurring in the key corresponding to Table 1.

Using the above key, Flipping key is determined. So the length of the Flipping key is 128 bit (i.e. 16×8 = 128). And using this key the substitution table and Inverse substitution Table 4 and 5 are also constructed. Though, we recognize that many important differences exist between watermarking and cryptographic security, a large part of the research is inspired by the Diffie-Helmann's paradigm, which is widely used in cryptography (Furon *et al*., 2001). The procedure is as follows:

The total number of ASCII Alpha-numeric values is 95. So, the substitution value ranges from 0-94. We need to substitute a value between 0-94 for each α-numeric character in the ASCII Table. The key K starting value 15 stands for the 15th Block in the Block table that has the following 4 special characters {|}- whose ASCII values are 123, 124, 125 and 126, respectively. So, we fill up the initial four values 0, 1, 2 and 3 for substitution table in those positions. The second key k value is 7. So, we go over to 7th block that contains H I J K L M whose ASCII values

Table 3: Block table

Block no.	Characters	No. of characters	Block no.	Characters	Block no.
1	Blank ! " # $ % & '	8	9	U V W X Y Z	6
2	( ) * + , - . /	8	10	[/] ^ _ `	6
3	0 1 2 3 4	5	11	a b c d e f g	7
4	5 6 7 8 9	5	12	h i j k l m	6
5	: ; < = > ? @	7	13	n o p q r s t	7
6	A B C D E F G	7	14	u v w x y z	6
7	H I J K L M	6	15	{ | } ~	4
8	N O P Q R S T	7			

Table 4: Substitution table

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

Table 5: Inverse substitution table

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

range 72-77. Hence, in substitution table they are the 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 123 for 0, 124 for 1, 125 for 2, 126 for 3 and so on.

Again this table is divided into subsets.

Permutation operation

Proposed folding technique: The origin of folding is from study folding (Kalaichelvi and Chandrasekaran, 2008) nature. This folding is broadly divided into 3 angles of processing:

- Horizontal folding
- Vertical folding
- Diagonal folding

Consider there are 5 rows present in the plain text document. Cipher text created with respect to the horizontal folding method finds the mid-row of whole text. With respect to that mid row, when is folded horizontally subsequent rows are exchanged as given in Cipher Text form (Fig. 2).

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

Fig. 2: Horizontal folding technique

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

Fig. 3: Vertical folding technique

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

Fig. 4: Diagonal vertical folding technique

In the case of vertical folding method columns are exchanged dynamically. It is same as horizontal folding using column processing instead of row processing (Fig. 3).

Exchange of rows/columns: 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 (Fig. 4).

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. However, we should be cautious with large values of the

encryption level since the increasing of the encryption level is proportional to the decreasing of the Encryption/ Decryption speed (William, 2008).

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.

The number of the flipping keys: There are 128 bits in a key. Each bit can be either 1 or 0. Therefore, there are 2^{128} flipping keys that make the algorithm invulnerable to brute force attack.

Description for watermarking technique: Digital watermarking is an effective way to protect copyright of multimedia data even after its transmission. A watermark embedded in the data, can uniquely identify the documents owner or authorized user (Alessandro and Bartolini, 2002).

Synchronization attacks like random cropping and time-scale modification are very challenging problems to audio watermarking techniques (Wei Li *et al*., 2003). This led to the image watermarking technique to embed the secret information that eliminates these problems (Fig. 5-7).

Module detailed design: The Algorithmic step to obtain the protected watermarked image after 3 levels, which embeds our secret information is described as:

Description of author module

Input: Image
Creation Unique Number (CUN)
Distributor Personal Identification Number (DPIN)
Author private key

Output: Transaction watermarked image

Processing: In this module Creation Unique Number (CUN) and Distributor Personal Identification Number (DPIN) is encrypted using author private key and the encrypted info is embedded into the image using transaction watermark embedder and all the information embedded into the watermarked image is decrypt and decoded using transaction watermark decoder.

Algorithm for author encryption:

- Read (Image)
- Read (CUN)

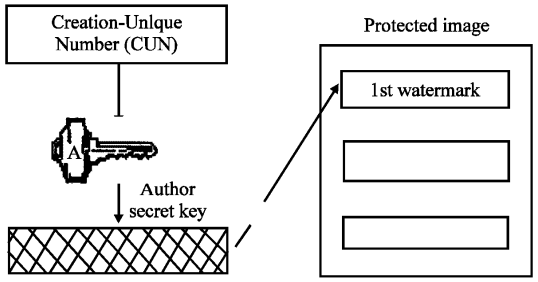

Fig. 5: First water marking in protected image

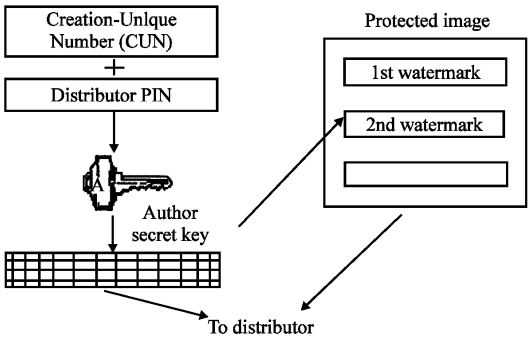

Fig. 6: Second water marking in protected image

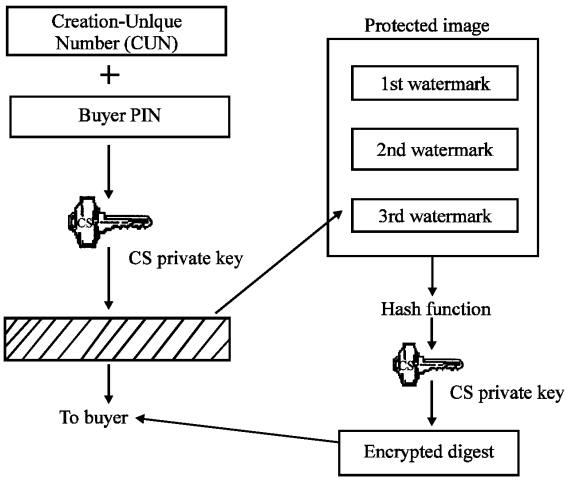

Fig. 7: Third water marking in protected image

- Read (DPIN)
- Compute the encrypted version of CUN and DPIN using author private key

$$\text{Cipher text } C = M^{e} (\text{Mod } n)$$

Where,

M = The original message
e = The author's private key
n = The nth field in author private key
C = Cipher text

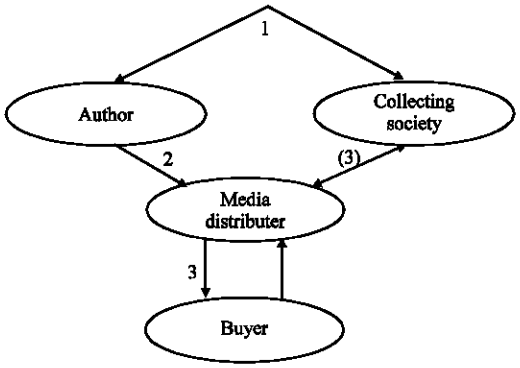

Fig. 8: Four modules of ECMS

Algorithm for transaction watermark embedding:

- Read (Image)
- Read (Encrypted_CUN)
- Compute the OFFSET value from image date
- Using Random access file option, we position the file pointer to OFFSET position
- Embed the encrypted info into the image

Description of collection society module:

Input: Authors public key
Collection Society (CS) private key
Buyer Personal Identification Number (PIN)
Watermarked image

Output: Watermarked image contain buyer PIN
encrypted string that contain third watermark

Proposed solution

Implementation details: This study consists of implementing the Electronic Copyright Management System (ECMS). In ECMS there are four modules (Fig. 8).

Author module: In this module CUN and Distributor PIN is encrypted using author private key and the encrypted info is embedded into the image using transaction watermark embedded. In this module, all the info embedded into the watermarked image is decrypt and decoded using transaction watermark decoder.

In the approach, the document is self-contained. At any given instant it contains all the information needed to verify whether, the current holder is using the data legally. No attempt is made to trace the document history, however, either by watermarking the document each time the owner changes, or by recording transaction details in a register. We take particular care to allow each actor to check that the data exchange was carried out correctly. The basic principle underlying our ECMS strategy is that the data holder's name must be watermarked into the data to prove legal ownership. To ensure that a document is being used legally, any authorized person can check the watermark field the holder's name is written in. We also, envision a protocol-level mechanism that addresses the reversibility problem by preventing data holders or counterfeiters from benefiting from watermark removal: at no step of the transaction can a counterfeiter insert a fake watermark, so a counterfeiter cannot prove document ownership. To keep misappropriating persons from writing their names into the data, the ECMS assumes that the seller (or the author when a media distributor sells the document) embeds the watermark.

Collection society module: In this module Buyer PIN and total document is encrypted using Collection Society (CS) private key. If author wants to sell copies of her document through a media distributor, she embeds a second watermark into the document. This watermark contains a Personal Identification Number (PIN) identifying the media distributor and the document's CUN. Author encrypts the watermark string with her private key and a copy of the encrypted string, which distributor can use to verify that author really inserted his name into the document. Distributor can use Author's public key to read the encrypted string and watermark detection software to verify it (Unlike with the first watermark, only an asymmetric cryptography scheme can be used here).

Buyer module: In this module, buyer verification is achieved by checking the watermarked string with the original watermark using watermark decoder.

String with encrypted third watermark is decrypted using Collection Society (CS) public key and the obtained CUN and Buyer PIN is compared

- BUYER passes his PIN to distributor
- Distributor passes buyer's PIN, the CUN and a string with the second watermark's content (that is, Distributor's PIN and the CUN encrypted with author's private key) to the CS
- The CS passes revenue to author
- After encrypting the string with buyer's PIN and the CUN with its private key, the CS embeds the second and the third watermarks into its copy of the document
- The CS computes a digest of the watermarked document using a proper hash function, signs the digest with its private key and sends the signed digest and the third, encrypted, watermark to distributor

- Distributor embeds the third watermark into the document and gives it, the encrypted third watermark and the signed digest to buyer

Verification process: To verify that Distributor has embedded his PIN within the data, Buyer need only decrypt the third watermark using the CS public key. To check whether, the CUN embedded in the third watermark corresponds to that in the first, Buyer can compute the digest of the watermarked document and confirm that it corresponds to the digest computed by the CS. Such a digest also allows buyer to verify the integrity of the watermarked document that is he can confirm that Distributor has not modified the original document.

Control authority module: This phase is used to verify the illegal usage. Protecting Data from Illegal Use Control authority asks buyer to prove his right to a digital document in its possession. Buyer can simply give the watermarked document and the file with the encrypted third watermark to the control authority. The CA first checks the encrypted.

Third watermark for buyer PIN, then, by applying a watermark detection engine to the protected document, it verifies that the watermark with buyer's PIN is actually embedded in the data. Finally, the CA, which knows both the true CUN and author's secret key can control whether, the CUN contained in the third watermark matches the document identity.

Indeed, the CA would not really need the user's file with the encrypted third watermark if it could get this information directly from the CS. Rather than storing all watermarking codes or digests, the CS can simply compute them, whenever it needs to, provided the CA gives it the required information. In particular, the CS can generate the second and third watermark and the digest, if it knows the media distributor's PIN, the buyer's PIN, the CUN and the author's identity.

RESULTS AND DISCUSSION

Here, the new variant FSP Algorithm developed has been adopted successfully to implement watermarking technique used for invisible information retrieval hidden in a picture message in ECMS.

At encryption level the newly developed FSP Algorithm helps to encrypt the incoming information and the spatial domain technique converts it into watermarked image is shown in the Fig. 9. The visible image now contains the secret information in invisible mode.

At decryption level the watermark decoding process, which again uses the FSP Algorithm gets back the secret

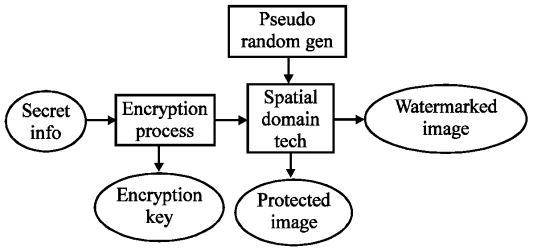

Fig. 9: Encoding with watermarking technique

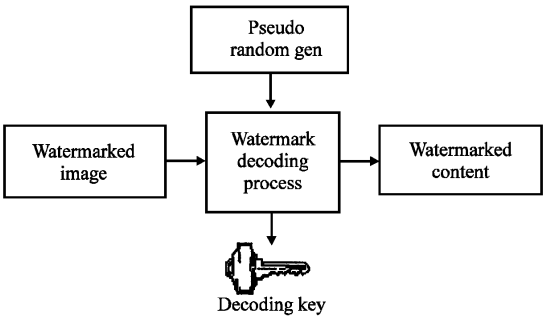

Fig. 10: Decoding with asymmetric watermarking technique

information in its original form. The decoding with asymmetric watermarking technique is illustrated shown in Fig. 10. The algorithm is fast as it uses 128 bits length flipping key and works fairly secure, since no unauthorized person can in anyway access the secret information as they require integrating application knowledge, which is available to only authorized and intended receivers.

CONCLUSION

This study addressed 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. Image file is transferred via LAN or email. This proposed scheme may further be enhanced and to be used in Copyright protection. In addition to that all the image formats should be supported by the software and the e-commerce used in e-transaction will be added in future. This software needs facility of Monitoring and analyzing intruders and raising

alarm with 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 (Richard, 2002). It is a simple concept that can fit transparently into existing communication applications.

ACKNOWLEDGEMENT

We are thankful B. Sankara Subramanian and S. Suriyanarayanan for his valuable guidance and discussions to carry out this research.

REFERENCES

Alessandro, P. and F. Bartolini, 2002. Copyright protection in open networks. IEEE. Internet Comput., 6 (3): 18-26. DOI: 10.1109/MIC.2002.1003126, PMID: 7317002. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1003126&isnumber=21649.

Bruce, S., 2001. Applied Cryptography. John Wiley and Sons Inc. 1st Edn. Hauz Khas, New Delhi, pp: 15-27. ISBN: 0-471-38922-6. http://www.amazon.co.uk/Applied-Cryptography-Protocols-Algorithms-Source/dp/0471117099.

Furon, T., I. Venturini and P. Duhamel, 2001. Unified Approach of Asymmetric Watermarking Schemes. 2002, Security and Watermarking of Multimedia Contents III. In: Wong, P.W. and E. Delp (Eds.). 4314: 269-279. DOI: 10.1109/MIC.2002.1003126. http://www2.computer.org/portal/web/csdl/doi/10.1109/MIC.2002.1003126.

Kalaichelvi, V. and R.M. Chandrasekaran, 2008. Proceedings of the International Conference on Computing and Communication Network (ICCCN), Karur, Tamilnadu, pp: 245-251. FSP Algorithm for encryption/decryption. Dec. 18-20 DOI: 10.1109/ICCCNET.2008.4787779. PMID: 10476732. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4787779.

Rade, P., 2003. Copyright Protection Based on Transaction Watermark. Telecommunications in Modern Satellite, Cable and Broadcasting Service, Vol. 2. San Diego, CA, USA. Oct. 1-3, pp: 509-518. ISBN: 0-7803-7963-2. DOI: 10.1109/TELSKS.2003.1246278. PMID: 8007683, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1246278&isnumber=27916.

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

Tsuhan Chen, Kou-Sou Kan and Ho-Hsun Chang, 2003. Watermarking 2D/3D Graphics for Copyright Protection. IEEE ICASSP, 4: IV-720-723. PMID: 7810434. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1202744.

Wei Li, Xiangyung Xue and Peizhong Lu, 2003. A Novel Feature-based Robust Audio Watermarking for Copyright Protection. Department of CSE, University of Fudan, Shangai, China, IEEE. Computers and Communication, Washington DC, USA, ISBN: 0-7695-1916-4,554-560.http://portal.acm.org/citation.cfm?id=845903.

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