ISSN 2277-3061

Digital Fingerprinting In Encrypted Domain

M.Kranthi Kumar[1], Dr.M.Kamaraju[2] , Dr.K.Ramanjaneyulu[3]
[1]Department of ECE, Gudlavalleru Engineering College, Gudlavalleru, India
E-mail id: kranthi.dhana@gmail.com
[2]Professor And HOD Department of ECE, Gudlavalleru Engineering College, Gudlavalleru, India
E-mail id: madduraju@yahoo.com
[3]Professor Department of ECE, PVP Siddhartha Institute of Technology, Vijayawada, India
E-mail id: ramaece406@gmail.com

ABSTRACT

Digital fingerprinting is a method for protecting multimedia content from illegal redistribution and identified the colluders.In copy protection, a content seller embeds a unique identity as a watermark into the content before it is sold to a buyer. When an illegal copy is found, the seller can identify illegal users by extracting the fingerprint. In this proposing an anonymous fingerprinting based on a homomorphic additive encryption scheme, it present a construction of anti-collision codes created using BIBD(Balanced incomplete block design) codes technique and dither technique which makes use of LFSR (linear feedback shift register) are used for improving the high robustness and Security.

Indexing terms/Keywords

Balanced Incomplete Block Design (BIBD) Coding, Digital Fingerprinting, Digital Cosine Transformation (DCT), Dither Technique, Liner Feedback Shift Register (LFSR).

Council for Innovative Research
Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol 12, No.1
editor@cirworld.com
www.cirworld.com, member.cirworld.com

ISSN 2277-3061

1. INTRODUCTION

Multimedia data protection is a major problem in digital world due to the easy of illegal redistribution through the Internet. In conventional fingerprinting schemes, the seller embeds the buyer's identity is a watermark into digital content. When the merchant encounters redistributed copies of this fingerprinted content, he can retrieve the identity information of the buyer and identified the particular person who (illegally) redistributed copy. In this scheme the identity information is known to the merchant, this enables a cheating merchant to embed the identity information of the buyer into any content without the buyer's consent and subsequently accuse the buyer of illegal redistribution [1].

Digital fingerprint [2] is a technique to detect unauthorized distributors of multimedia content by embedding a unique identifying code in each legally distributed copy.The unique copies where as in fingerprint a unique code is embedded for each customer. The illegal distributor can be identified by extracting the fingerprint from the illegally distributed multimedia identifying code (fingerprint) can be embedded using watermarking or any other secure embedding technique, which is robust. The fundamental difference between watermarking and fingerprinting is that, in watermarking same data is embedded in all the distributed copy.

Digital fingerprinting the unauthorized distribution is prevented and authenticity is achieved by the insertion of the fingerprint. It is analogous with human fingerprint, where the purpose is only to identify a specific person. No other characteristics of the person can be revealed. Likewise, digital fingerprint can be used to identify a particular person, but no other characteristics of the multimedia can be explained. The fingerprint is unique to the user purchasing the media data, so that illegal distributors can be caught using these fingerprints.

An illegal distributor will try to escape from identification through fingerprinting by implementing a collusion attack where a group of users combine their copies in order to make an image with modified fingerprint. An efficient fingerprint system should be developed in such a way that it can support a large number of users (database capacity) and can effectively resist a collusion attack (robustness). If we look at both the digital fingerprinting process and the collusion attack process collectively, then the complete system may be viewed as consisting of three main parts: fingerprint embedding, collusion attacks and fingerprint detection. The Balanced Incomplete Block Design (BIBD) based codes are very popularly used as fingerprint codes since these codes have good robustness and capacity [3][5].

In fingerprinting schemes, the identity information is embedded into the digital data by the merchant and the fingerprinted copy is given to the buyer. When the seller (merchant) encounters redistributed copies of this fingerprinted content, he can retrieve the identity information of the buyer who (illegally) redistributed his copy. From the buyer point of view, this is unattractive because during the embedding procedure, the merchant obtains the identity information of the buyer, this enables a cheating merchant to embed the identity information of the buyer into any content without the buyers consent and subsequently accuse the buyer of illegal redistribution [6].

In this paper to protect the identity of the buyer, anonymous fingerprinting schemes have been proposed [7, 8], In [9], the buyer and the merchant follow an interactive embedding protocol, in which the identity information of the buyer remains unknown to the merchant. When the buyer wishes to purchase, for instance, an image, he registers himself to a registration centre and receives a proof of his identity with a signature of the registration centre. Then the buyer encrypts his identity and sends both encrypted identity and the proof of identity to the merchant. The merchant checks the validity of the signature by using the public key of the registration centre. After the buyer convinces the merchant, through the provided identity proof, that the encrypted identity indeed contains the identity information of the buyer, the merchant embeds the identity information of the buyer into the (encrypted) image data by exploiting the homomorphic property of the cryptosystem. Then the encrypted fingerprinted image is sent to the buyer for decryption and future use. We present a construction of collusion-resistant fingerprints based up on BIBD codes technique, the merchant embeds the identity information of the buyer into the (encrypted) image data by exploiting the homomorphic property of the cryptosystem and anonymous fingerprinting protocol as shown in below figure(1).

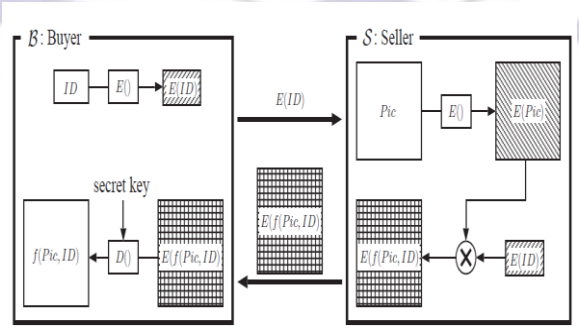


Figure 1: The flow of anonymous fingerprinting protocol

In this scheme, the merchant can only retrieve the identity information of the buyer when it is detected in a copy of the fingerprinted image. This idea,first presented in [22], was constructed in [21, 24] using digital coins. In order to embed the identity information of the buyer, a single-bit commitment scheme with exclusive or homomorphism, is used that allows for computing the encrypted XOR of two bits by multiplying their cipher texts. In [8, 9] , this construction is not efficient because of the low enciphering rate. The single bit commitment scheme can only contain one bit of information for a $\log_2 n$

bit cipher-text, where `n' is a product of two large primes.In order to increase the enciphering rate, using a cryptosystem with a larger message space. They introduced an anonymous fingerprint algorithm based on an additive homomorphic cryptosystem that allows for the addition of values in the plaintext domain by multiplying their corresponding ciphertexts.In order to increase the enciphering rate, Kuribayashi and Tanaka suggested using a cryptosystem with a larger message space. They introduced an anonymous fingerprinting algorithm based on an additive homomorphic cryptosystem that allows for the addition of values in the plaintext by multiplying their corresponding ciphertexts. The embedding positions were already known to the merchant, so that fingerprint can be retrieved back when an illegal copy is obtained.

2 TYPES OF DIGITAL FINGERPRINTING

There are two types of digital fingerprinting depends on colluder detection ability and size of the database (number of users) (1) Orthogonal fingerprinting (2) Coded fingerprinting.

2.1 Orthogonal fingerprinting

One important method for digital fingerprinting is suggested by Trappe and Liu. They tried to improve the collusion resistance of fingerprinting system by introducing the concept of orthogonal modulation where orthogonal fingerprint codes are used. The orthogonality or independence allows distinguishing the fingerprints to the maximum extent. Simplicity of encoding and embedding orthogonal fingerprints make them attractive to applications involving a small group of users [10-16].

The disadvantages with orthogonal fingerprinting scheme are the maximum number of users that can be supported by an orthogonal fingerprinting system is equal to the dimension of the fingerprint. To increase the number of users the dimension of the fingerprint code also has to be increased proportionally. The energy of the fingerprint signals get reduced during the collusion. Under linear collusion, this becomes significant and detection problem arises. The third disadvantage with this scheme is the computational complexity associated with estimating which user's fingerprint is present, when the total number of users is large. This is because the number of correlations to be computed is proportional to the number of users [20]. For a large group of users, this leads to significant detection complexity [23].

2.2 Coded Fingerprinting

An approach to counteract the energy reduction due to collusion using orthogonal codes is to introduce correlation between the fingerprint codes. Further, by introducing correlation, dependence among the fingerprint codes can be introduced and more number of fingerprints can be obtained, than the dimensionality of the fingerprint. The challenge is to design these fingerprints so that they have good anti-collision properties. There are three types of codes available in order to make the fingerprinted copy. They are (1) Collusion Secure codes (2) Anti Collusion codes (AND-ACC) (3) BIBD codes (Balanced Incomplete Block Design).

2.2.1 Collusion Secure Codes

A primitive binary code that consists of n possible code words of length(n – 1). For the m^{th} codeword, the first (m − 1) bits are 0 and the rest are 1. According to the marking assumption, by inspecting the primitive code, the colluders will not be able to detect the first (m – 1) bits, hence the first (m – 1) bits will remain "0" after collusion. If the detector observes that the first (m – 1) bits are 0 and the m^{th} bit is a 1, then we can conclude that user m was involved in the collusion. But there is no guarantee that the colluders will switch the bit to a "1," which prompts the need for some method to encourage a "1" showing up during collusion.

This is accomplished by repetition and permutation techniques. Repetition and permutation help hide which position of the digital object encodes which fingerprint bits. But since each of them has the same value at all six positions, they would not know which three out of the six bits correspond to the first three bits before permutation, and which correspond to the second three bits. As a result, they cannot alter the underlying Γ_0 (4, 3) code at will. Based on the principle that every colluder should contribute an equal share to the colluded data, some of the six bits would be set to "1" and others to "0." A detector starts from the first block and examines each block in a block-by-block manner, which is analogous to the bit-by-bit examination of the primitive code. The number of "1"s per code block is used as an indicator of a user's involvement in collusion [17-19].

2.2.2 Anti Collusion Codes(Acc*)*

An anti-collusion code (ACC) is a family of code vectors for which the bits shared between code vectors uniquely identifies groups of colluding users. ACC codes have the property that the composition of any subset of K or fewer code vectors is unique. This property allows for the identification of up to K colluders. In order to identify colluders, we require that there are no repetitions in the different combinations of K or fewer code vectors. The codes that satisfy this property are called ACC.

To improve the performance of the collusion secure codes, anti collusion codes can be proposed based on orthogonal code modulation. The marking assumption in the CS code is replaced by combinatorial design and enhanced by accumulation of pseudo noise (PN) codes called Anti Collusion Code (ACC).AND-ACC achieves better performance in colluder detection. . We want to design codes such that when K or fewer users collude, we can identify the colluders. Shorter codes are preferred for embedded fingerprints because longer codes would distribute the fingerprint energy over more basis vectors, which would lead to a higher error rate in the detection process [15-18].

A binary code C {c_1, c2 …cn} such that the logical AND of any subset of `k' or fewer code vectors is non-zero and distinct from the logical AND of any other subset of k or fewer code vectors is a k-resilient anti-collusion code. An example of a K-Resilient Anti-Collusion Code, when n = 4 is C= {1110, 1101, 1011, 0111}. It is easy to see when k≤ n-1 of these vectors are combined under logical AND, each combination is unique. In given example n = 4. Let c1= (1110), c2=(1101), c3=(1011) and c4=(0111). Logical AND Codes resulting for different combinations of k≤3 are for k=2 c_1,c_2 = (1100), c_1,c_3 = (1010), c_1,c_4 = (0110), c_2, c_3 = (1001), c_2,c_4 = (0101), c_3,c_4 = (0011) and for k = 3 c_1,c_2, c_3 = (1000), c_1, c_2, c_4 = (0100), c_2,c_3,c_4 = (0001). Anti-collusion codes can be used with code modulation to construct a family of fingerprints with the ability to identify colluders.

2.2.3 Construction Of Bibd-Based Acc

In coded fingerprinting, CDMA-type modulation is used in which for each user a pn sequence is modulated using a unique binary code for each user. These unique binary codes are generated to be collusion-resistant using the theory of balanced incomplete block designs (BIBD) and the resulting fingerprints are termed anti-collision codes.

A(v,k,**λ**) BIBD code is a set of k-element subsets (blocks) of a v-element set X ,such that each pair of elements of X occur together in exactly **λ** blocks. Each element of X appears in exactly `r' blocks. The `incomplete' in the name of BIBD refers to the condition v > k, i.e., the block size `k' is less than the total number of treatments, so no block contains all the varieties or elements. If we allowed v = k, then all the conditions would be trivially satisfied and the resulting design would not be of much interest. Balanced refers to the constancy of the λ parameter. BIBD's are often referred to as (v, b, r, k, λ) designs or simply (v, k, λ**)** designs. A (v, k, **λ**) BIBD has a total of n **=** λ (v^2 - v)/ (k^2 -k) blocks.

A (v, k, λ) BIBD code can be represented using an v n incidence matrix `M', where each element M (i, j) is set to `1' when the i^{th} element belongs to the j^{th} block, and set to `0' otherwise, the corresponding (k-1) resilient ACC code vectors can be obtained as the bit complements of the columns of the incidence matrix of a (v, k, 1) BIBD. The code vectors are therefore v-dimensional, and are able to accommodate n = (v^2-v)/(k^2-k) users with these v basis vectors. Assuming that a BIBD exists, for n users and a given collusion resiliency of (k-1), need v = O($\sqrt{n}$) basis vectors are needed.

For example, consider a (7, 3, 1) BIBD code. Let X = {1, 2, 3, 4, 5, 6 ,7} be the set from which we are creating BIBD, `k' is taken as 3 i.e, each block contains exactly 3 varieties. For a BIBD to function as anti-collusion codes, must be equal to 1. The BIBD subsets obtained according to the given conditions is given by C = {124, 136,157, 235, 267, 347, 456}, r=repetition number which can be considered as `3', for example the element `1' is repeated thrice, and =1 in BIBD code construction i.e, each pair of varieties appear simultaneously in exactly 1 block. We can represent a (v, k, λ) BIBD design, with a v b matrix called the incidence matrix of the design. If i^{th} variety is contained in block j then the (i , j)th element is represented as 1. Each block is represented as a column vector. The presence of a variety in each block is denoted by zero and absence is denoted by one. Putting all column vectors together, we will obtain the following matrix. If we use the antipodal form of code modulation, each column vector **c** of **C** will be mapped to {+/- 1} by $f(x) = 2x - 1$.Let u_1,u_2….u_7 represents the basis vectors. The fingerprint signal is constructed as a linear combination of set of orthogonal basis signals {u_j} as

$$\mathbf{w} = \sum_{j=1}^{v} f(c_j)\boldsymbol{u}_j$$

3 HOMOMORPHIC ENCRYPTION

Succeeding works showed that some asymmetric cryptosystems preserve structure, which allows for arithmetic operations to be performed on encrypted data. This structure preserving property, called homomorphism, comes in two main types, namely, additive and multiplicative homomorphism. Using additive homomorphic cryptosystems, performing a particular operation (e.g., multiplication) with Encrypted data, results in the addition of the plaintexts. Similarly, using a multiplicatively homomorphic cryptosystem, multiplying ciphertexts, results in the multiplication of the plaintexts [7, 8]. Cryptosystems are broadly classified as two types namely Public key cryptosystem, Private key cryptosystem.

3.1 Public Key Cryptosystem

The public key cryptography, Alice and Bob need only exchange their public keys, without concern as to eavesdropping, before they can communicate privately. This allows secure communication between parties with no prior acquaintance or communication and without the need for a secure means of key transfer. Further, in a party of *n* users desiring pair wise privacy, each user must keep only one secret key and *n* keys must be made publically available to all users. By contrast, using private key cryptography each user must keep n-1 secret keys, with a total of n^2-n secret keys having to be generated and securely transferred. The difference in difficulty of key management is thus quite significant. With the advent of public key cryptography, cryptography moved out of its former exclusive domain of government or military use and is today widely used by corporations of all sizes as well as by individuals.

Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and the other is public. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions by itself. The public key may be published without compromising security, while the private key must not be revealed to anyone not authorized to read the messages. Public-key cryptography uses asymmetric key algorithms and can also be referred to by the more generic term \asymmetric key cryptography." The algorithms used for public key cryptography are based on mathematical relationships that presumably have no efficient solution. Although it is computationally easy for the intended recipient to

generate the public and private keys. To decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult (or effectively impossible) for anyone to derive the private key.

3.2 Private Key Cryptosystem

Private key cryptosystem is also known as Symmetric-key cryptosystem. Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher-text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. The two keys in this cryptosystem are used for both encryption as well as decryption.

3.2.1 Encryption

In cryptography, encryption is the process of encoding messages (or information) in such a way that third parties cannot read it, but only authorized parties can read it. Encryption doesn't prevent hacking but it prevents the hacker from reading the data that is encrypted. In an encryption scheme, the message or information (plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext . This is usually done with the use of an encryption key.

Okamoto and Uchiyama proposed a semantically secure and probabilistic public key cryptosystem based on composite numbers. Let $n = {}^{p2q}$, where p and q are two prime numbers of length k bits, and let g be a generator such that the order of $g = (p-1) \bmod p^2$ is p. Another generator is defined as $h = gn$. In this scheme, the public key is $pk = (n, g, h, k)$ and the secret key is $sk = (p, q)$ [1] [15-19].

A message m ($0 < m < 2^{k-1}$) is encrypted as follows:

$$c = E(m, r) = g^m h^r \bmod n$$

Where r is a random number.

3.2.2 Decryption

Decryption is the reverse operation of encryption. This is the process of converting ciphertext back to plaintext. Decoding the cipher-text is defined as

$$m = D(c) = (L(c^{p-1} \bmod n) \div L(g^{p-1 \bmod})) \bmod p$$

Where the function $L(\cdot)$ is

$$L(u) = (u-1) \div p$$

It has the additive homomorphic property such that, given two encrypted messages E (m1,r1)and E (m2,r2), the following equality holds.

$$E(m_1, r_1) \times E\, m_2, r_2) = E(m_1 + m_2, r_1 + r2)$$

Here x denotes integer modulo-n multiplication.

4 COMPRESSION TECHNIQUES

Compression refers to reducing the quantity of data used to represent a file, image or video content without excessively reducing the quality of the original data. It also reduces the number of bits required to store and transmit digital media. To compress something means that decrease its size. There are different techniques available. In this we explain mainly two techniques (1) Huffman coding (2) Run length coding.

4.1 Huffman Coding

Huffman coding is an entropy encoding algorithm mainly used for lossless data compression. The term refers to encoding a source symbol (such as a character in a file) use a variable length code table, where the variable-length code table has been derived in a particular way based on the estimated probability of occurrence for each possible value of the source symbol. It uses a specific method for choosing the representation for each symbol, resulting in a prefix code that expresses the most common source symbols using shorter strings of bits than are used for less common source symbols. The Huffman algorithm is mainly based on statistical coding, which means that the probability of a symbol has a direct bearing on the length of its representation. More probable of occurrence of a symbol have shorter will be its bit size representation. In any file, certain characters are used more than the others. Using binary representation, the number of bits required to represent each character depends upon the no. of characters that have to be represented. Using one bit we can represent two characters, i.e., ‘0’ represents the first character and ‘1’ represents the second character. Using two bits we can represent four characters.

`A',`B',`C',`D',`E' having their frequencies are 24,12,10,8,8 respectively. The two rarest symbols `E' and `D' are connected first, followed by `C' and `B'. The new parent nodes have the frequency 16 and 22 respectively and are brought together in the next step. The resulting node and the remaining symbol `A' are subordinated to the root node that is created in a final step. A character's code is found by starting at the root and following the branches that lead to that character.

4.2 Run Length Coding

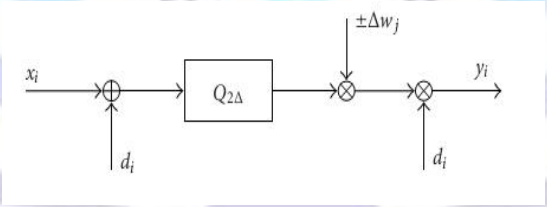
It is the simplest method of compression compared to other compression techniques. Run length is defined as the number of consecutive equal values. It is used for compressing data that contains repeated values and is performed after Huffman coding. Both Huffman coding and run length coding are reversible. Before applying run length coding we should make sure that the sequence to be encoded should have repeating values. If the sequence doesn't contain any repeatingvalues, the length of the compressed data will be twice that of the original. Starting with the first value of input it is compared with the next value and if it is equal to the previous value, a counter is incremented by 1; otherwise the previous value followed by the run length `1' is output. For example, let `111000110000001' be the sequence to be encoded. The run length output is `1303120611'.

5 PSEUDO RANDOM SEQUENCE GENERATION

We need to go for dither technique which makes use of LFSR (linear feedback shift register) or PN sequence (pseudo random sequence) generator. A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state bits. The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the sequence of values produced by the register is completely determined by its current (or previous) state. The LFSR is having finite number of possible states so that it would enter a repeating cycle [19]. An LFSR with a well chosen feedback function can produce a sequence of bits which appears random i.e., PN sequence. An LFSR is a shift register that, when clocked, advances the signal through the register from one bit to the next most significant bit. A linear feedback shift register can be formed by performing exclusive-OR on the outputs of two or more of the flip-flops together and feeding those outputs back into the input of one of the flip-flops. Linear feedback shift registers make extremely good pseudorandom pattern generators. When the outputs of the flip-flops are loaded with a seed value (anything except all 0s, which would cause the LFSR to produce all 0 patterns) and when the LFSR is clocked, it will generate a pseudorandom pattern of 1s and 0s. Note that the only signal necessary to generate the test patterns is the clock.

Working of Linear Feedback Shift Registers sequence through2^n-1states, where 'n' is the number of registers in the LFSR. At each clock edge, the contents of the registers are shifted right by one position. There is feedback from predefined registers or taps to the left most register through an exclusive-NOR (X-NOR) or an exclusive-OR (X-OR) gate. A value of all "1"s is illegal in the case of a X-NOR feedback. A count of all "0"s is illegal for an XOR feedback. This state is illegal because the counter would remain locked-up in this state. The LFSR is implemented with X-OR feedback. A 4-bit LFSR sequences through (2^4-1) = 15 states (the state 1111 is in the lock-up/illegal state). A 4-bit binary up-counter would sequence through 2^4 = 16 states with no illegal states. LFSR counters are very fast since they use no carry signals. However, the dedicated carry in Vertex devices is rarely a speed limiting factor because it is intrinsically fast. LFSRs can replace conventional binary counters in performance critical applications where the count sequence is not important (e.g., FIFO). LFSRs are also used as pseudo-random bit stream generators.

From the perspective of the seller, the embedding of the buyer's identification information must be as robust as possible in order to both withstand malicious and benign signal-processing operations on the fingerprinted signal. So in order to increase the robustness a dither technique is used. In dither technique, a PN- sequence is added before embedding the watermark in quantized samples; later on this sequence would be subtracted by the same PN-sequence generated by LFSR. The figure 2 shows how dither is added to quantized samples, where "d_i" is the dither generated by PN-sequence.



Figuer 2: . Dither technique

6 SIMULATION RESULT

6.1 Fingerprinting In Plane Domain

In fingerprinting schemes, the identity information is embedded into the digital data by the merchant in user one (fig.4) and user two (fig.5) from original copy (fig.3), the fingerprinted copy is given to the buyer. When the merchant encounters illegally (redistributed) copies of this fingerprinted content, he can extracted the identity information of the illegally (redistributed) copy as shown in (fig.6). The average of correlation values is known as threshold value, when correlation value is more than threshold value collusion done, so identify the colluder. From the buyer point of view, this is unattractive because during the embedding procedure, the merchant obtains the identity information of the buyer, this enables a cheating merchant to embed the identity information of the buyer into any content without the buyers consent and subsequently accuse the buyer of illegal redistribution.To protect the buyer identity we have to go for anonymous fingerprinting.

Fig (3).Original image

Fig (4).Fingerprinted image for user one

Fig (5).Fingerprinted image for user two

Fig (6).colluded copy

Table 1.Exctracted fingerprints from illegal copy using fingerprinting scheme.

Fingerprint for user one	1 1 1 1 0 0 1 0
Fingerprint for user two	1 1 1 1 0 0 0 0
Extracted code	-10.4529 -10.4517 -10.4562 -10.4467 -10.2955 -10.3063 -10.3415 -10.3299
Threshold value	-10.3851
Colluder is	1 1 1 1 0 0 0 0

The fingerprinted values user one, user two are embedded in to digital images. Extracted and threshold values of colluded copy as shown in table.1.

6.2 Fingerprinting In Encrypted Domain

In anonymous fingerprinting embedding scheme is done in encrypted domain, the buyer encrypts fingerprint and embedding fingerprint in user one(fig.8) and user two(fig.9) from original copy (fig.7) send it to the seller. The encryption and decryption process are done using public and private keys. Buyer receives the encrypted fingerprinted copy and decrypted using private key.If the correlation value is above a particular threshold that user is identified as a colluder as shown in fig.(10). Threshold value is taken as the average of computed correlations. The equation for computing the correlation is given by

$$T_N = \mathbf{y}^T \mathbf{s} / \sqrt{\sigma_d^2 \cdot \|\mathbf{s}\|^2}$$

Where T_N denotes the correlation vector, y is the extracted fingerprint signal and s denotes the basis vector.

Fig (7).Original image

Fig (8).User one

Fig (9).User two

Fig (10).colluded copy

Table.2 Extracted fingerprints from illegal copy using anonymous fingerprinting scheme.

Fingerprint for user one	1 1 0 0 0 0 1 0
Fingerprint for user two	1 1 0 0 0 0 0 1
Decimal equivalent of image taking 3 bits in a group:	3 0 0 0 0 0 0 7
Decrypted values:	4 1 0 0 0 0 0 8
Extract code after collision attack	4 1 0 0 0 0 0 4
Colluder is:	1 1 0 0 0 0 0 1

As indicated above table.2 encryped and decrypted values are shown,comparisation of correlation values for different users as show in below table.3 and identify colluder.

Table.3 comparison the correlation values for three or more users are present.

Colluded data	Correlation value for different users(T)			Persons identified as colluder
	User1	User2	User3	
User 1 and 2	0.9923	0.9892	0.8788	1 and 2
User 2 and 3	0.9078	0.9191	0.9946	2 and 3
User 3 and 1	0.9042	0.9028	0.9961	3 and 1
User 1,2 and3	0.9405	0.9421	0.9839	1,2 and 3

7 CONCLUSION:

In conventional fingerprinting schemes, the buyer's identity is known to the merchant during embedding. This knowledge can be easily abused by a malicious merchant by creating fingerprinted copies containing this identity information without the buyer's consent. After distribution, the merchant can claim a license violation for this specific buyer. To deal with this problem, this proposed a reasonably efficient solution based on embedding the buyer identification information using additive homomorphic encryption schemes. This anonymous fingerprinting scheme is implemented in this work. To increase the robustness, dither technique generated by Linear Feedback Shift Register is used in this work.

REFERENCES

[1] J. P. Prins, Z. Erkin, and R. L. Lagendijk *"*Anonymous Fingerprinting with Robust QIM Watermarking Techniques" *Hindawi Publishing Corporation EURASIP Journal on Information Security, Volume* 2007, Article ID 31340, 13 pages doi:10.1155/2007/31340.

[2] N. Memon and P. Wong, "A buyer-seller watermarking protocol,"*IEEE Transactions on Image Processing*, vol. 10, no. 4, pp.

[3] Min Wu, Wade Trappe, Z. Jane Wang, and K.J. Ray Liu "*collusion-resistant fingerprinting for multimedia"* IEEE Signal Processing Magazine1053-5888/04/$20.00©2004.

[4] M. Wu and B. Liu, "Data hiding in image and video: Part-I—Fundamental issues and solutions," *IEEE Trans. Image Processing*, vol. 12, pp. 685–695, June 2003.

[5] J.G. Proakis, "Digital Communications"*,* 4th ed*.* New York: McGraw-Hill, 2000.

[6] Z. Jane Wang, Min Wu, Hong Vicky Zhao, Wade Trappe, and K. J. Ray Liu*, "*Anti-Collusion forensics of multimedia Fingerprinting usin Orthogonal modulation*", IEEE transactions on Image processing*, vol. 14, no. 6, pp.804 – 821, June 2005.

[7] Dan Boneh and James Shaw, "Collusion-Secure Fingerprinting for Digital Data"*, IEEE transactions on* information theory, vol. 44, no. 5, pp 1897 – 1905, September 1998.

[8] Wade Trappe, MinWu, JaneWang, K. J. Ray Liu, "Anti-collision Fingerprinting for Multimedia", *IEEE transactions on Signal Processing,*vol. 51, no. 4, pp1069 –1087, April 2003.

[9] Shu Lin, Daniel.J.Costello, "Error control coding, Fundamentals and Applications"*, Pearson Education*, Second Edition, 2004.

[10] Abhiram Prabhakar, Krishna Narayanan, "Pseudo Random Construction Of Low Density Parity Check Codes using Linear Congruential Sequences",*IEEE Transactions on communication*, vol.50, no.9, September, 2002, pp.1389-1396.

[11] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, "Overview on Selective Encryption of Image and Video: Challenges and Perspectives"*, EURASIP Journal on Information Security*, pp 5-7, 2008.

[12] Z. JaneWang, MinWu, Wade Trappe, K. J. Ray Liu, "Group-Oriented Fingerprinting for Multimedia Forensics", *EURASIP Journal on Applied Signal Processing*, pp 2142–2162, 2004.

[13] Ross Anderson, Charalampos Manifavas, *Chameleon* -A New Kind of Stream Cipher*, Proceedings of Fast Software Encryption Workshop*, pp 107-113, 1997.

[14] shiguo Lian, Dimitris Kanellopoulos, Giancarlo Ruffo, "Recent Advances in multimedia information security*", Informatica* 33,pp 3-24,2009.

[15] Shan He, Min Wu, "Joint Coding and Embedding Techniques for Multimedia Fingerprinting*", IEEE transactions on information Forensics and security*, vol. 1, no. 2, pp 231-247, June 2006.

[16] N. R.Wagner, "Fingerprinting," in Proc. Symp. Security Privacy, Oakland,CA, pp. 18–22, Apr. 1983.

[17] Alexander Barg, G. R. Blakley, And Grigory A. Kabatiansky*, "*Digital Fingerprinting Codes: Problem Statements, Constructions, Identification of Traitors", *IEEE transactions on information theory*, vol. 49, no. 4, pp 852-865,april 2003.

[18] A. N. Lemma, S. Katzenbeisser, M. U. Celik, M. V. Veen, "Secure Watermark Embedding Through Partial Encryption*", Proceedings of International Workshop on Digital Watermarking* (IWDW 2006), Springer LNCS, 4283, 433-445, 2006.

[19] P. Kitsos, N. Sklavos, N. Zewas and 0. Koufopavlou *"*A reconfigurable linear feedback shift register(LFSR)*", IEEE international conference on Digital Object Identifier*, vol.2 , Page(s): 991 – 994,2001.

[20] Wu, M., Trappe, W., Wang, Z. J. & Liu, K. J. R. "Collusion resistant fingerprinting for multimedia", IEEE Signal Processing Mag. pp. 15.

[21] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Transactions on Image Processing, vol*. 14, *no.* 12, *pp.* 2129– 2139, 2005.

[22] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," *in International Conference on the Theory and Application of Cryptographic Techniques (EU-ROCRYPT* '98), *vol*. 1403, *pp*. 308–318, *Espoo, Finland, June* 1998.

[23] P. Kitsos, N. Sklavos, N. Zewas and 0. Koufopavlou *"A reconfigurable linear feedback shift register(LFSR)",* IEEE international conference on Digital Object Identifier, vol.2 , Page(s): 991 – 994,2001.

[24] L. M. Cheng, L. L. Cheng, C. K. Chan, and K.W. Ng, "Digital watermarking based on frequency random position insertion," presented at Control, Automation, Robotics and Vision Conference,vol. 2, pp. 977-982, 2004.