SECURE SYSTEM BASED ON RECOMBINED FINGERPRINTS FOR SHARING MULTIMEDIA FILES IN PEER TO PEER NETWORKS

D.Amu[1], C.Roselinmary[2], M.Priya[3], S.Vaishnavi[4]

[1]*Assistant professor, Dept of Information Technology, Alpha College of Engineering & Technology, Pondicherry*
[2]*B.Tech Student, Dept of Information Technology, Alpha College of Engineering & Technology, Pondicherry*
[3]*B.Tech Student, Dept of Information Technology, Alpha College of Engineering & Technology, Pondicherry*
[4]*B.Tech Student, Dept of Information Technology, Alpha College of Engineering & Technology, Pondicherry*

Abstract

In this paper the execution time is less when compared to previous algorithm. And also it provide security between the merchant and buyer The traitor tracing protocol is used to detect the illegal transaction. Here we used fingerprinting solution to avoid illegal redistribution of multimedia contents. Here we convert the multimedia video file into image then encrypting the image after the encrypted image will be transferred from merchant to buyer. The buyer receives the copyright protection from merchant, he decrypts the image then converts it into video. After that, the copyright protection of file is transferred to child buyer. Then tracing traitor protocol is used to checks the fingerprints for merchant to buyer and buyer to child buyer. Traitor tracing protocol is used to detect the illegal transaction of the content. The Blowfish algorithm is used to encrypt and decrypt the multimedia files. Finally we detect the performance of our work based on efficiency, accuracy and we achieve security.

Keywords: *Fingerprint, Multimedia files, Blowfish algorithm, Merchant, Buyer, Child Buyer, Copyright Protection*

----------***----------

1. INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions.

It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name i.e. the password this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used. Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS. help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wireshark traffic and may be logged for audit purposes and for later high-level analysis. Fingerprinting emerged as a technological solution to avoid illegal content re-distribution. Basically, fingerprinting consists of embedding an imperceptible mark –fingerprint– in the distributed content to identify the content buyer. The embedded mark is different for each buyer, but the content must stay perceptually identical for all buyers. Fingerprinting schemes deter people from illegally redistributing digital data by enabling the original merchant of the data to identify the original buyer of a redistributed copy. Recently, asymmetric fingerprinting schemes were introduced. Here, only the buyer knows the fingerprinted copy after a sale, and if the merchant finds this copy somewhere, he obtains a proof that it was the copy of this particular buyer. In case of illegal re-distribution, the embedded mark allows the identification of the re-distributor by means of a traitor tracing system, making it possible to take subsequent legal actions. Although fingerprinting techniques have been available for nearly two decades, the first few proposals in this field are far from nowadays' requirements such as scalability for thousands or millions of potential buyers and the preservation of buyers' privacy.

Most fingerprinting systems can be classified in three categories, namely symmetric, asymmetric and anonymous schemes. In symmetric schemes, the merchant is the one who embeds the fingerprint into the content and forwards the result to the buyer; hence, the buyer cannot be formally accused of illegal redistribution, since the merchant also had access to the fingerprinted content and could be responsible for the redistribution. In asymmetric fingerprinting, the merchant does not have access to the fingerprinted copy, but he can recover the fingerprint in case of illegal re-distribution and thereby identify the offending buyer. In anonymous fingerprinting, in addition to asymmetry, the buyer preserves her anonymity (privacy) and hence she cannot be linked to the purchase of a specific content, unless she participates in an illegal re-distribution. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application.

They are said to form a peer-to-peer network of nodes. Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Emerging collaborative P2P systems are going beyond the era of peers doing similar things while sharing resources, and are looking for diverse peers that can bring in unique resources and capabilities to a virtual community thereby empowering it to engage in greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers. Many anonymous fingerprinting schemes exploit the homomorphic property of public-key cryptography. These schemes allow embedding the fingerprint in the encrypted domain (with the public key of the buyer) in such a way that only the buyer obtains the decrypted fingerprinted content after using her private key. Other approaches for anonymous fingerprinting do not exploit homomorphic encryption in this way, but either 1) require highly demanding technologies such as public-key encryption of the contents, secure multiparty protocols, commitment protocols or zero-knowledge proofs, among others, incurring prohibitive computational and communicational costs; or 2) are based on theoretical secure embedding algorithms for which no proof of existence is available.

2. RELATED WORK

2.1 Rational Peer to Peer

The authors **J.Domirgo-Ferror and D.Megias** proposed this “Distributed multicast of fingerprinted content based on a rational peer-to Peer community”. In conventional multicast transmission, one sender sends the same content to a set of receivers. This precludes fingerprinting the copy obtained by each receiver (in view of redistribution control and other applications). A straightforward alternative is for the sender to separately fingerprint and send in unicast one copy of the content for each receiver. This approach is not scalable and may implode the sender. We present a scalable solution for distributed multicast of fingerprinted content, in which receivers rationally co-operate in fingerprinting and spreading the content. Furthermore, fingerprinting can be anonymous, in order for honest receivers to stay anonymous. This paper focuses on proposing a multicast approach to the anonymous fingerprinting problem which meets these two goals and shows a proof of concept with a practical implementation of the proposed system. The idea is to transfer the burden of a centralized fingerprinting technology to a distributed network of buyers who will collaborate to produce further copies of the fingerprinted contents.

The solution guarantees the following properties: Correctness: All protocols terminate successfully whenever players are honest (no matter how other players behaved in other protocols). Anonymity and unlinkability: Without obtaining a particularDB, the merchant even when colluding with the registration center– cannot identify a buyer (anonymity). Furthermore, the merchant is not able to tell whether two purchases were made by the same buyer (unlinkability). Revocability and collusion resistance: Any collusion of up tocbuyers aiming at producing a version b D2Dfrom which none of them can be re-identified will fail: frombDthe merchant will obtain enough information to identify at least one collusion member. The content carries a different anonymous fingerprint for each receiver, so that unlawful content redistribution can be tracked ; honest receivers stay anonymous. The sender does not need to fingerprint and send the content individually to each receiver; one fingerprinting and one unicast transmission by the server to one collaborative receiver are enough to bootstrap the process.

The advantages aided in this method are time domain synchronization watermark is embedded for fast search of information watermark position.A frequency-domain information watermark is embedded next to the SYN marks.Disadvantage of our proposed peer-peer multicast protocol only deals with the redistribution control.

2.2 Spread Spectrum Fingerprinting in Asymmetric Cryptographic Protocol

The author **M.Kuribayashi** Proposed this “On the Implementation of Spread Spectrum Fingerprinting in Asymmetric Cryptographic Protocol.Asymmetric Property If both a buyer and a seller obtain a fingerprinted content in a fingerprinting protocol, the seller cannot prove to a third party about the illegal distribution by the buyer, even if the buyer's fingerprint is extracted. This is because the seller may distribute it himself in order to frame an innocent buyer. Hence, it is desirable that only a buyer is able to obtain his own fingerprinted content in the protocol. Such a protocol is called asymmetric fingerprinting protocol. We propose the method for implementing the spread spectrum watermarking technique by carefully designing parameters for rounding operation. If frequency components of digital

contents are used for the embedding fingerprint information, they must be quantized in order to truncate real value to integer. Then, the precision of the frequency components should be considered in order not to degrade a watermarked image. When the spread spectrum watermarking technique in is applied, the precision of the representing watermark signal is sensitive for the implementation. By scaling up the parameters by multiplying a constant factor, the precision is increased in our scheme. Then, the trade-off between the scaling factor and the amount of data to be transmitted must be considered. In addition, for the characteristic of the fingerprinting protocol, frequency components and the watermark signal must be separately encrypted after quantization. In such a case, the consistency of the precision is a sensitive issue. Since an embedding operation is performed by addition of frequency components and a spread spectrum sequence, the additive homomorphic property of public-key cryptosystems can be directly exploited for the embedding. Then, the separate rounding operation causes interference term in a deciphered data at a buyer side. Without loss of secrecy of an original content, the interference term is removed after decryption. The performance of our proposed method is evaluated comparing with the conventional scheme, which conrms the similar identification capability of illegal buyers. In a fingerprinting scheme, each fingerprinted copy is slightly different, hence, malicious users will collect some copies with respective watermark in order to remove/alter the watermark. Collusion-secure code which has traceability of colluders.In the watermarking algorithm, it consists of Embedding and Decryption and Post-Processing.
Advantages is the embedding operation can be easily performed using the additive homomorphic property of public-key cryptosystems such as the Okamoto-Uchiyama encryption scheme. Disadvantages is we can simulate the scheme on the cryptographic protocol with a limited precision.

3. EXISTING SYSTEM

3.1 Security Model

The security assumptions of the systems are the following:
The merchant does not need to be trusted the either for distribution or to associate a pseudonym with the identity of the buyer. Buyers are not trusted and protocols are provided to guarantee that 1. They are transferring authenticated fragments of contents. 2. Their anonymity can be revoked incase of illegal re-distribution.

The transaction monitor will not have access to the clear text of the fingerprints. This prevents that any single party single party can frame an innocent buyer.

The transaction monitor is trusted as the symmetric keys used for encrypting the fragments. This means that the Transaction monitor stores the key provided by each parent buyer and this key can be retrieved only once from its database.The transaction monitor returns the true pseudonym corresponding to an illegal re-distributor in the traitor tracing protocol. This trust can be replaced by a collection of signatures provided by the proxies. The tracing authority is a part of the legal system and shall be trusted the communication between the merchant and the seed buyer and between the peer buyers within the P2P distribution system must be anonymous using an onion routing- like approach. The fragments of content are encrypted using symmetric cryptography. The proxies are not trusted and the fragments sent through them shall be encrypted in such a way that only the sender and the recipient have access to their clear text.

The multimedia content is divided into several fragments and each of the fragments is embedded separately with a random binary sequence. The binary sequence of each fragment is called segment and the concatenation of all fragments forms the whole fingerprints. The merchant distributes the different copies to the seed buyer and fingerprints of this buyer. After that the buyer receives the fragments from seed buyer. Then the communication between the peer buyers is anonymous through onion routing-like protocol using a proxy. Proxies know the pseudonyms of source and destination buyers and they have access to the symmetric keys used for encrypting the multimedia content. Transaction record is created by transaction monitor to keep track of each transfer between peer buyers. These records do not contain the fingerprints, but only an encrypted hash of them. The fingerprints' hashes are encrypted in such a way that the private key of at least one parent is required for obtaining their clear text. The real identities of buyers are known only by the merchant.

3.2 Peer to Peer Distribution Protocol

In the original distribution protocol the fingerprints were not stored in the traitor tracing monitor in order to protect the privacy of the buyer. Only the hash of the fingerprint was stored for each buyer. The fingerprint's hash was encrypted and stored as many times as parents each buyer each buyer had, using the public key of the parent for encryption. The transaction registers would be formed as follows:
$P_{i\ -->}$ Username of the buyer
H(c)-> Perceptual content hash
$E_{hi->}$ Encrypted hash of the buyer's fingerprint.
$E_{fi->}$ Encrypted buyer's fingerprint.
d-> Transaction date and time.

the transaction monitor stores the following encrypted version of the fingerprint:

$$Efi = E\ (E^{c}_{g1}\ |E^{c}g2\ |\ldots.E^{c}_{gm}, K_a\ )\ |\ldots..|\ E\ (E^{c}_{g(L\text{-}1)m+2}\ |\ E^{c}_{g(L\text{-}1)m+2}\ |\ldots|E^{c}_{gLm}, K_a\ ).\backslash$$

3.3 Algorithm Description

DES algorithm used in previous work. It uses 64 bit block cipher and it encrypts 64 bit data at a time. DES uses the two basic techniques of cryptography - confusion and diffusion. At the simplest level, diffusion is achieved through numerous permutations and confusions is achieved through the XOR operation. The execution time is slow in DES algorithm.

4. PROPOSED SYSTEM

To overcome the problems in the existing system, here we include so many improved measures. In our proposed system the components we are going to include are Merchant, seed buyers, other buyers, proxies, tracing authority and transaction monitor. The work of the merchant is that he distributes copies of the content legally to the seed buyers. Each fragment of the content contains a different segment of the fingerprint embedded into it. The segments have low pair-wise correlations. The work of seed buyers is they receive fingerprinted copies of the contents from the merchant that are used by the P2P distribution system to bootstrap the system. The works of other buyers are they purchase the content and obtain their fingerprinted copies from the P2P distribution system. The content is assembled from fragments obtained from different parents. Anonymous connections with peer buyers are provided by means of proxies. The duties of proxies are they provide anonymous communication between peer buyers by means of a specific protocol analogous to Chaum's mix networks. The work of tracing monitor is it keeps a transaction register for each purchase carried out for each buyer. This transaction register includes an encrypted version of the embedded fingerprints. The work of tracing authority in case of illegal re-distribution, it participates in the tracing protocol that is used to identify the illegal re-distributor(s).The watermarking method used for embedding and detecting the fingerprint is transparent, robust and secures enough for a fingerprinting application. Collusion occurs when several buyers decide to recombine their fingerprinted copies of a given content trying to obtain a new copy in which neither of their fingerprints is detectable. Buyer frameproofness is related to the possibility that an innocent buyer is accused of illegal redistribution of the purchased content.

Advantages

- Our proposed system improves the efficiency of the fingerprinted system
- It also preserves the privacy of the original copy of the multimedia file
- It effectively detects the traitors who are all misuse the original copy of multimedia file.
- It uses the recombined fingerprints for validation, so it generates the effective result.

4.1 Comparison between DES and Blowfish

Algorithm	Block size	Bits	Time consumption	Execution time
DES	64 bits	64 bits	Low	high
Blowfish	64 bits	32 to 448 bits	High	low

4.2 System Modules

- Data distribution
- Fingerprinted copies to seed buyers
- Distribution to other buyers
- Transaction Monitoring
- Traitor tracing protocol

4.2.1 Data Distribution

In the data distribution process, it first identify the merchant information. That is full details about the merchant, merchant id, etc. After that merchant should select the multimedia file which they going to send to the buyers. In the process, the name of the multimedia file, type of the multimedia file and extension of the multimedia file finally size of the multimedia file are displayed. After that in a client server process they transmit the merchant information and the contents they are going to send to the buyers are viewed. Finally the buyers who are all take part in this file sharing process are viewed. Here we select the final selection of buyer and merchant information.

4.2.2 Fingerprinted Copies to Seed Buyers

After the analyzing process, the copies are ready to send to the buyers. Before the transmission process, we are going to encrypt the copies. In this process we are going to convert the multimedia file into number of copies of images. After that view the information about the images we convert during the first process. Finally we encrypt the images using AES algorithm. Using the encryption algorithm we encrypt the images which we converted during the conversion process. Finally send the encrypted image copies to the seed buyers.\

4.2.3 Distribution to Other Buyers

The encrypted copies are first received to the seed buyers. After the copies are received at the seed buyers, these copies are ready to send to the other buyers. In the middle process, the copies are converted into the binary values. This binary value is mainly used for the validation process. These binary values are the fingerprints of the copies of the video files. There are separate fingerprint is generated for the each and every copies send to the seed buyers, from the seed buyers to the other buyers. Here we show the binary values of the fingerprints of the copies of the multimedia files are viewed.

4.2.4 Transaction Monitoring

In the transaction monitoring it contains the record of each and every transaction. That is the copy of the multimedia file send from one peer to another peer, the ip of the sender peer and receiver peer are recorded in the transaction monitoring. This transaction monitoring is helpful to identify the illegal distribution of multimedia file copies to the peer involved in the network. It is like a register which contains the information about all the peers and transactions etc After that we show all the transaction information about the peers takes part in the network.

4.2.5 Traitor Tracing Protocol

It is a final step, in this module it detects the tracing of the illegal distributors. In case of illegal re-distribution, it participates in the tracing protocol that is used to identify the

illegal re-distributor(s).By referring the transaction monitor, it detect the illegal distribution of videos among the merchant and the seed buyers.

4.3 Proposed Algorithm Description

Blowfish algorithm is a symmetric block cipher key. It is used for encryption. It takes a variable-length key, from 32 bits to 448 bits. Blowfish is unpatented and license free algorithm. Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encrypted. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. It manipulates data in large blocks. It has a scalable key from 32 bits to at least 256 bits. It has no linear structures that reduce complexity. Blowfish has 16 rounds. The input is a 64-bit data element, X. It divides X into 32-bit halves: XL , XR

Then, for i=1 to 16:

$$XL = XL \text{ XOR } Pi$$

$$XR = F(XL) \text{ XOR } XR, \text{ Swap XL and XR}$$

4.4 Architechture Diagram

The below figure describes, merchant send video file that file encrypted into segments. Then the buyer provides their fingerprints to merchant. After that the buyer decrypts the file . The blowfish algorithm is used for encryption process. The buyer's information stored in tracing monitor. The tracing monitor used to store database of buyers. And hashed fingerprints. The tracing protocol is used to detect illegal transaction in peer to peer network.

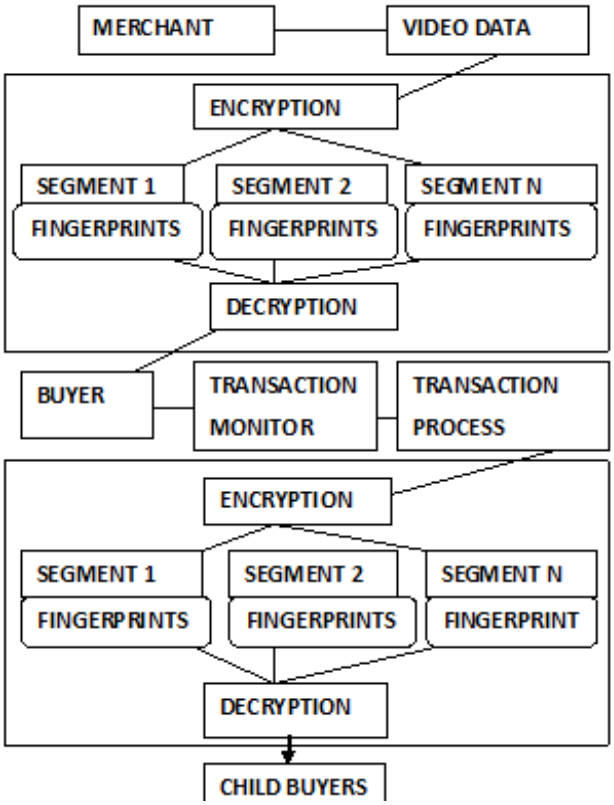

Fig1.1 Architechture diagram

5. PERFORMANCE METRICS

The graph defines to compare the execution time between the DES and blowfish algorithm. When comparing these algorithms the execution time of blowfish is fast.The execution finished in earl time. In our improved measure uses the blowfish algorithm for encrypting the file. The blowfish algorithm is easy to encrypt the file.

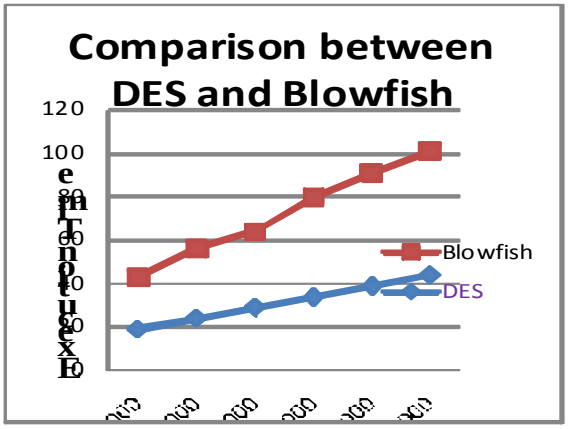

Fig 1.2 Comparison of execution time

6. CONCLUSION AND FUTURE WORK

Merchant did not kno about the fingerprint of the buers. Some of the the buyers fingerprints are embedded and others fingerprints are obtained from the recombination. This paper shows that the co-operation of honest buyers in traitor tracing entails several relevant drawbacks that can make the

published system fail under some circumstances. Tracing authority identify the illegal redistribution of data. And the correct users can get the data without any interruption. If any unwanted distribution is made the traitor tracing protocol detects the illegal re-distribution of the content. Future work in our project will change the algorithm concept for execution process or change the protocol to detect illegal transaction.

REFERENCES

[1]. D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," Advances in Cryptology-CRYPTO'95, LNCS 963, Springer, pp. 452-465, 1995.

[2]. Y. Bo, L. Piyuan, and Z. Wenzheng, An efficient anonymous fingerprinting protocol. Computational Intelligence and Security, LNCS 4456, Springer, pp. 824–832, 2007.

[3]. J. Camenisch, "Efficient anonymous fingerprinting with group signatures," Asiacrypt 2000, LNCS 1976, Springer, pp. 415–428, 2000.

[4]. C.-C. Chang, H.-C.Tsai, and Y.-P. Hsieh, "An efficient and fair buyer-seller fingerprinting scheme for large scale networks," Computers & Security, vol. 29, pp. 269–277, Mar. 2010.

[5]. D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, pp. 84–90. Feb. 1981.

[6]. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Burlington MA: Morgan Kaufmann, 2008.

[7]. J. Domingo-Ferrer and D. Meg´ıas, "Distributed multicast of fingerprinted content based on a rational peer-to-peer community," Computer Communications, vol. 36, pp. 542–550, Mar. 2013.

[8]. M. Fallahpour and D. Meg´ıas, "Secure logarithmic audio watermarking scheme based on the human auditory system," Multimedia Systems, in press.

[9]. S. Katzenbeisser, A. Lemma, M. Celik, M. van der Veen, and M. Maas, "A buyer-seller watermarking protocol based on secure embedding," IEEE Trans. on Information Forensics and Security, vol. 3, pp. 783–786, Dec. 2008.

[10]. M. Kuribayashi, "On the implementation of spread spectrum fingerprinting in asymmetric cryptographic protocol," EURASIP Journal on Information Security, vol. 2010, pp. 1:1–1:11, Jan. 2010.

[11]. C.-L. Lei, P.-L.Yu, P.-L.Tsai, and M.-H. Chan: An efficient and anonymous buyer-seller watermarking protocol. IEEE Transactions on Image Processing, vol. 13, pp. 1618–1626, Dec. 2004.

[12]. D. Meg´ıas and J. Domingo-Ferrer, "DNA-Inspired Anonymous Fingerprinting for Efficient Peer-To-Peer Content Distribution," Proc. 2013 IEEE Congress on Evolutionary Computation (CEC 2013), pp. 2376–2383, Jun. 2013.

[13]. D. Meg´ıas and J. Domingo-Ferrer, "Privacy-aware peer-to-peer content distribution using automatically recombined fingerprints," Multimedia Systems, in press.

[14]. N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. on Image Processing, vol. 10, pp. 643–649, Apr. 2001.

[15].PandoNetworks.http://www.pandonetworks.com/p2p.

[16]. B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," Advances in Cryptology-EUROCRYPT'97, LNCS 1233, Springer, pp. 88–102, 1997.

[17]. B. Pfitzmann and A.-R.Sadeghi, "Coin-based anonymous fingerprinting," Advances in Cryptology-EUROCRYPT'99, LNCS 1592, Springer, pp. 150–164, 1999.

[18]. R. O. Preda and D. N. Vizireanu, "Robust wavelet-based video watermarking scheme for copyright protection using the human visual system," Journal of Electronic Imaging, vol. 20, pp. 013022– 013022-8, Jan.-Mar. 2011.

[19]. J. P. Prins, Z. Erkin, and R. L. Lagendijk, "Anonymous fingerprinting with robust QIM watermarking techniques," EURASIP Journal on Information Security, vol. 2007, pp. 20:1–20:7, Dec. 2007