Overview of watermarking and cryptography to combine both for real time speech communication

Bhumi Patel[1], Prof. R C Patel[2]

***Abstract*—Both encryption and digital watermarking techniques need to be incorporated in a speech communication to address different aspects of speech content management. While encryption transforms original multimedia object into another form, digital watermarking leaves the original object intact and recognizable. The objective of research is to develop FPGA base real time, reliable and secure watermarking systems, which can be achieved through hardware implementations. Data-size is one of the major concerns of cryptographic systems. This development also includes speech compression to overcome the effect of data rate increase due to addition of watermarking and decryption key. Based on this research we can also say about the effect of compression on data quality. Protocol in MATLAB and FPGA will be developed which will perform various tasks at same time like, accept speech data, compression, watermarking, and encryption. Another protocol for receiver will receives that signal data, decrypts signal, remove watermark and apply interpolation to retrieve original speech data. For this implementation first we require to study various algorithms for watermarking, encryption and data compression which will best suitable for our application. This review paper gives information about various techniques for speech watermarking and data encryption.**

***Keywords*—cipher, cryptography, decryption, encryption, FPGA, watermarking.**

I. INTRODUCTION

A digital watermark is a digital signal or pattern inserted into a digital speech or image. Since this signal or pattern is present in each unaltered copy of the original data, the digital watermark may also serve as a digital signature for the copies [1]. A given watermark may be unique to each copy (e.g. to identify the intended recipient), or be common to multiple copies (e.g. to identify the document source). In either case, the watermarking of the document involves the transformation of the original into another form. This distinguishes digital watermarking from digital fingerprinting, where the original file remains intact and a new created file 'describes' the original file's content.

Encryption is said to occur when data is passed through a series of mathematical operations that generate an alternate form of that data; the sequence of these operations is called an algorithm. To help distinguish between the two forms of data, the unencrypted data is referred to as the plaintext and the encrypted data as cipher text. The security of encryption lies in the ability of an algorithm to generate cipher text that is not easily reverted to the original plaintext. In a very simple example, encryption of the word "secret" could result in "terces." Reversing the order of the letters in the plaintext generates the cipher text. This is a very simple encryption - it is quite easy for an attacker to retrieve the original data. There are two main requirements for cryptography:

1. It should be computationally infeasible to derive the plaintext from the cipher text without knowledge of the decryption key.

2. It should be computationally infeasible to derive the cipher text from the plaintext without knowledge of the encryption key.

Both these conditions should be satisfied even when the encryption and decryption algorithms themselves are known.

Watermarking and encryption are both used to ensure data confidentiality. However the main difference between them is that with encryption anybody can see that both parties are communicating in secret. Watermarking hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. This makes watermarking suitable for some tasks for which encryption isn't, such as copyright marking. Adding encrypted copyright information to a file could be easy to remove but embedding it within the contents of the file itself can prevent it being easily identified and removed.

II. CRYPTOGRAPHY VS WATERMARKING

Before moving towards the types of algorithm it's important to understand the difference between cryptography and watermarking. Below table-1 shows the difference between cryptography and watermarking for different criteria.

III. WATERMARKING REQUIREMENTS

In this section, we study a number of watermarking system requirements as well as the tradeoffs among them.

- **Security:**

The security requirement of a watermarking system can differ slightly depending on the application. Watermarking security implies that the watermark should be

Manuscript received January 27, 2014.

***Bhumi Patel**, post graduate student, Instrumentation and control engineering department, L D college of engineering, Gujarat technological university, Ahmedabad, Gujarat, India. Mobile No-9925954566*

***Rakesh C Patel**, Professor, Instrumentation and control engineering department, L D college of engineering, Gujarat technological university, ,Ahmedabad, Gujarat, India*

ISSN: 2278 – 7798

difficult to remove or alter without damaging the host signal. As all watermarking systems seek to protect watermark information, without loss of generality, watermarking security can be regarded as the ability to assure secrecy and integrity of the watermark information, and resist malicious attacks [18].

- **Imperceptibility:**

The imperceptibility refers to the perceptual transparency of the watermark. Ideally, no perceptible difference between the watermarked and original signal should exist [19, 20].A straightforward way to reduce distortion during watermarking process is embedding the watermark into the perceptually insignificant portion of the host signal [20].However, this makes it easy for an attacker to alter the watermark information without being noticed.

- **Capacity:**

Watermarking capacity normally refers to the amount of information that can be embedded into a host signal. Generally speaking, capacity requirement always struggle against two other important requirements, that is, imperceptibility and robustness. A higher capacity is usually obtained at the expense of either robustness strength or imperceptibility, or both.

- **Robustness:**

Watermark robustness accounts for the capability of the watermark to survive signal manipulations. Apart from malicious attacks, common signal processing operations can pose a threat to the detection of watermark, thus making it desirable to design a watermark that can survive those operations. For example, a good strategy to robustly embed a watermark into an image is to insert it into perceptually significant parts of the image. Therefore, robustness is guaranteed when we consider the case of lossy compression which usually discards perceptually insignificant data, thus data hidden in perceptual significant portions is likely to survive lossy compression operation. However, as this portion of the host signal is more sensitive to alterations, watermarking may produce visible distortions in the host signal. The exact level of robustness an algorithm must possess cannot be specified without considering the application scenario [21]. Not all watermarking applications require a watermark to be robust enough to survive all attacks and signal processing operations. Indeed, a watermark needs only to survive the attacks and those signal processing operations that are likely to occur during the period when the watermarked signal is in communication channel. In an extreme case, robustness may be completely irrelevant in some case where fragility is desirable.

IV. TYPES OF WATERMARKING

In the literature large number of text [22], image [23], audio [24] and video [25] watermarking algorithms can be found. These algorithms modify the original media to generate the watermarked media. There may be no or little perceptible differences between the original media and the watermarked media. Fig.1 gives an overview of different types of watermarking methodologies depending on their working domains, cover media, perceptibility and application areas.

Speech Watermarking can be split into two types, these are Fragile and Robust. The following section describes the definition of these two different types of watermarking.

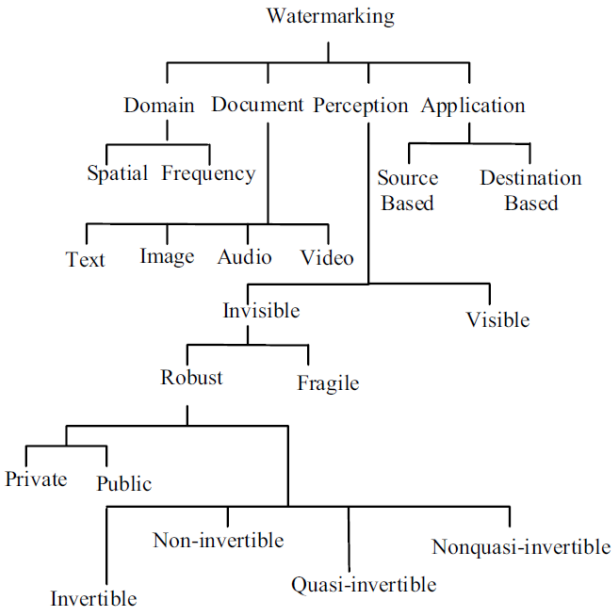

Fig.1 Different types of watermarking methodologies

- **Fragile Watermarking**

A watermark is said to be fragile if the watermark hidden within the host signal is destroyed as soon as the watermarked signal undergoes any manipulation. When a fragile watermark is present in a signal, we can infer, with a high probability, that the signal has not been altered. Fragile watermarking authentication has an interesting variety of functionalities including tampering localization and discrimination between malicious and non-malicious manipulations. Tampering localization is critical because knowledge of where the speech data has been altered can be effectively used to indicate the valid part of the speech data, to infer the motive and the possible adversaries. Moreover, the type of alteration may be determined from the knowledge of tampering localization.

As to the fragile watermarks for authentication and proof of integrity, the attacker is no longer interested in making the watermarks unreadable. Actually, disturbing this type of watermark is easy because of its fragility. The goal of the attackers is, conversely, producing a fake but legally watermarked signal. This **host media forgery** can be reached by either making undetectable modifications on the watermarked signal or inserting a fake watermark into a desirable signal.

Now, it is necessary to formulate the unique features of fragile watermarking systems in order to demonstrate what features are well sought after. The features can also serve in theoretical analysis for making comparisons among algorithms:

ISSN: 2278 – 7798

1) **High resolution tampering localization:** This becomes an important merit of fragile watermarking systems as it is one of the features that makes watermarking outweighs cryptography in some applications. The outcome of a detector can be as simple as authentic/tampered, but a result indicating which portions in an image are tampered is more desirable.

2) **Tampering detection with low false positive**. A good fragile watermarking system should have a sound tamper indication stating both statistical tampering probability and tampering localization with a low false positive rate. If the tampering localization is required to be accurate, the false positive rate must be kept low or localization resolution is compromised. For example, the boundary of tampered region may be obscure when false positive rate is not low enough, even if block size is small.

3) **Geometric manipulation detectability.** The watermark should be correctly read by the detector in the intact portions after geometric manipulations such as image cropping. Further, the ability of the detector to indicate where the cropping took place is of crucial importance in some applications.

4) **Attack identification.** With proper settings, the detector is also able to estimate what kind of modification had occurred to an attacked image. This includes the ability to differentiate geometric attacks from other attacks. It implies that cropping a part of the image will not result in disturbing the whole watermark.

5) **Proper embedding sequence.** It implies that the selection of dependency is limited to the previously watermarked portion of the image. If localization is required, the dependency information for the to-be-watermarked pixel can only be chosen from the neighboring pixels from the dependency selection. Because the to-be-watermarked pixel can only depend on the content information that will not be changed later, otherwise the watermark will not be recognized by the detector. Raster-scan and zig-zag scan order are both widely used [26].

6) **Blind detection.** For practicality, watermark detectors should not require an original copy, or there would be no necessity for watermarking as the verification can be performed by simply comparing the received image with the original one. The watermark extraction should naturally be blind for practicality.

- **Robust Watermarking**

Robust marking aims to embed information into a file which cannot easily be destroyed. Although no mark is truly indestructible, a system can be considered robust if the amount of changes required to remove the mark would render the file useless. Therefore the mark should be hidden in a part of the file where its removal could be easily perceived. There are two main types of robust marking. Fingerprinting involves hiding a unique identifier for the customer who originally acquired the file and therefore is allowed to use it. Should the file be found in the possession of somebody else, the copyright owner can see the fingerprint to identify which customer violated the license agreement by distributing a copy of the file. Unlike fingerprints, watermarks identify he copyright owner of the file, not the customer. Whereas fingerprints are used to identify people who violate the license agreement watermarks help with prosecuting those who have an illegal copy. Ideally fingerprinting should be used but for mass production of CDs, DVDs, etc it is not feasible to give each disk a separate fingerprint.

Watermarks are typically hidden to prevent their detection and removal, they are said to be imperceptible watermarks. However this need not always be the case. Visible watermarks can be used and often take the form of a visual pattern overlaid on an image. The use of visible watermarks is similar to the use of watermarks in non-digital formats (such as the watermark on currency notes).

V. Purpose of Cryptography

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- *Authentication:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography and public-key (or asymmetric) cryptography, each of which is described in next section. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *ciphertext*, which will in turn (usually) be decrypted into usable plaintext.

VI. Types of Cryptography (Encryption Algorithms)

The cryptography algorithms are divided into two groups: symmetric-encryption algorithms and asymmetric-encryption algorithms. When using symmetric

ISSN: 2278 – 7798

algorithms, both parties share the same key for encryption and decryption. To provide privacy, this key needs to be kept secret. Once somebody else gets to know the key, it is not safe anymore. Symmetric algorithms have the advantage of not consuming too much computing power. A few well-known examples are: DES, Triple-DES (3DES), IDEA, CAST5, BLOWFISH, and TWOFISH.

Asymmetric algorithms use pairs of keys. One is used for encryption and the other one for decryption. The decryption key is typically kept secretly, therefore called "private key"' or "secret key", while the encryption key is spread to all who might want to send encrypted messages, therefore called "public key". Everybody having the public key is able to send encrypted messages to the owner of the secret key. The secret key can't be reconstructed from the public key. The idea of asymmetric algorithms was first published 1976 by Diffie and Hellmann.

Asymmetric algorithms seem to be ideally suited for real-world use: As the secret key does not have to be shared, the risk of getting known is much smaller. Every user only needs to keep one secret key in secrecy and a collection of public keys, which only need to be protected against being changed. With symmetric keys, every pair of users would need to have an own shared secret key. Well-known asymmetric algorithms are RSA, DSA, ELGAMAL.

However, asymmetric algorithms are much slower than symmetric ones. Therefore, in many applications, a combination of both is being used. The asymmetric keys are used for authentication and after this has been successfully done; one or more symmetric keys are generated and exchanged using the asymmetric encryption. This way the advantages of both algorithms can be used. Typical examples of this procedure are the RSA/IDEA combination of PGP2 or the DSA/BLOWFISH used by GnuPG. Figure-2 shows the field of cryptography. Some of the widely used algorithms are discussed in detail.

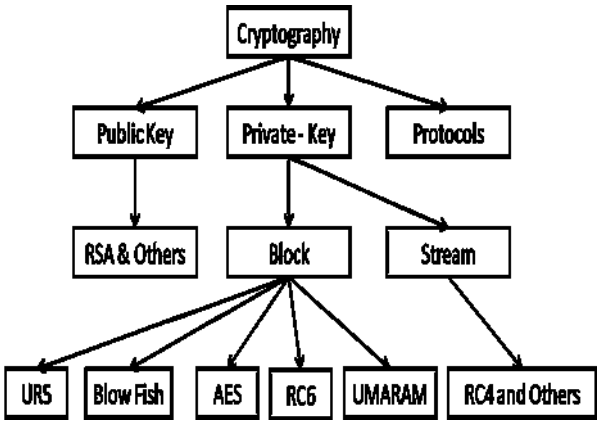

Fig.2 Overview of the field of Cryptography

There are a lot of symmetric-encryption algorithms used in general, such as DES [28], ThreeDES, RC6 [31], UMARAM [32], RC2 and UR5 [30]. In all these algorithms, both sender and receiver have used the same key for encryption and decryption processes respectively. The outside attackers use the fixed plaintext and encrypted text to obtain the key used in the WLAN. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [29]. Brief definitions of the most common symmetric encryption techniques are given as follows:

- **DES:** (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).DES is (64 bits key size with 64 bits block size) .Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [28].

- **Triple DES:** 3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods [26].

- **RC2:** RC2 is a block cipher with a 64-bits block cipher with a variable key size that range from 8 to128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts [27].

- **RC6:** RC6 is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard [31].

- **UMARAM:** The UMARAM Algorithm [32] is a new symmetrical encryption algorithm was designed by G.Ramesh and R. Umarani in the year 2010. The UMARAM is a Symmetrical encryption algorithm. The key generation generates 16-keys during 16-rounds.One key of them is used in one round of the encryption or decryption process. The new algorithm uses a key size of 512-bits to encrypt a plaintext of 512-bits during the 16-rounds. In this Algorithm, a series of transformations have been used depending on S-BOX, different shift processes, XOR-Gate, and AND-Gate. The S-Box is used to map the input code to another code at the output. It is a matrix of16×16×16 .The S-Box consists of 16-slides, and each slide having 2-D of16×16. The numbers from 0 to 255 are arranged in random positions in each slide.

- **UR5:** The UR5 Algorithm [30] is a new symmetrical encryption algorithm was designed by Ramesh and Umarani in the year 2011. .A block encryption algorithm is UR5 in this approach. In this Algorithm, a series of transformations have been used depending on S-BOX, XOR Gate, and AND Gate. The UR5 algorithm encrypts a plaintext of size 64-bits by a key size of 64-bits. It uses eight rounds for encryption or decryption process. It overcomes some drawbacks of the other algorithms.

There are several asymmetric algorithms in existence today, including RSA, DSA, ElGamal, and ECC. Currently, the most popular is RSA, which stands for Rivest, Shamir, and Adelman, the names of its inventors.

- **RSA**: is a widely used cryptosystem in the world. It is a public key cryptosystem which uses two kinds of key, private key and public key. Every user has both of the keys, a private one and a public one. If user A wants to

ISSN: 2278 – 7798

send a message to B, he need B's public key to encrypt the message. After encrypted, the message is received by B, then B uses his private key to decrypt the message.

- **DSA**, which was proposed by NIST in 1991, stands for Digital Signature Algorithm. DSA is somewhat less flexible, since it can be used for digital signatures but not for confidentiality or symmetric key exchange.

- **The ElGamal algorithm**, which was invented by Taher ElGamal, is based on the problem of calculating the discrete logarithm in a finite field. The ElGamal Algorithm provides an alternative to the RSA for public key encryption. 1) Security of the RSA depends on the (presumed) difficulty of factoring large integers.2) Security of the ElGamal algorithm depends on the (presumed) difficulty of computing discrete logs in a large prime modulus. ElGamal has the disadvantage that the cipher text is twice as long as the plaintext. It has the advantage the same plaintext gives a different cipher text (with near certainty) each time it is encrypted.

- **ECC** stands for Elliptic Curve Cryptography, which was independently proposed in 1985 by Neal Koblitz and V. S. Miller. EEC is not actually an algorithm, but an alternate algebraic system for implementing algorithms, such as DSA, using peculiar mathematical objects known as elliptic curves over finite fields.

Some asymmetric algorithms, such as RSA and ElGamal, can be used for both encryption and digital signatures. Other asymmetric algorithms, such as DSA, are useful only for implementing digital signatures. It is also generally true that asymmetric algorithms tend to be much slower and less secure than symmetric algorithms for a comparable key size. To be effective, asymmetric algorithms should be used with a larger key size, and, to achieve acceptable performance, they are most applicable to small data sizes. Therefore, asymmetric algorithms are usually used to encrypt hash values and symmetric session keys, both of which tend to be rather small in size compared to typical plaintext or speech data.

VII. Future work

The goal of this review paper is to give an idea about watermarking and cryptography. In future based on these studies we like to develop a real time working system for speech communication using FPGA which performs secure speech transmission with watermarking. Based on study we will find the best suitable algorithms for watermarking and cryptography which we can combine together to implement in hardware. A new FPGA hardware-based secured audio communication scheme for real-time speech signal will be developed which can be used for identification, ownership verification and authentication. This system could use for many applications where secured and authenticated speech communication is required for example in future this system can be use for ATM machines where secured transactions required with bank watermark . Also we like to focus to combine compression algorithm with watermarking and cryptography which will help to overcome to the problem of increase in data rate due to watermark and encryption key insertion in original speech data.

VIII. Conclusion

In this paper we have discussed basic of watermarking and cryptography. Also we tried to focus to differentiate watermarking and cryptography. Various algorithms available for the speech watermarking and encryption are discussed. Depending upon the different parameters required for the watermarking and encryption we can select the appropriate method to combine both which helps to develop an algorithm for can secure speech transmission with watermarking. Based on hardware implementation complexity, security criteria and data rate problem, we found that combination of Robust Watermarking and RC6 encryption algorithm is best suitable for real time speech communication. This combination can be implement in FPGA based hardware for real time speech communication.

REFERENCES

[1] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu, "A comparative Analysis of Image Steganography", *International Journal of computer Applications* (0975-8887), May, 2010, Vol 2, No. 3.

[2] Bret Dunber, "Steganographic Techniques and their use in an Open-Systems Environment", *SANS Institute*, 01/18/2002.

[3] D. Aucsmith, "An information-theoretic model for steganography", Proceedings of the second Intel. *Workshop on Information Hiding*, April, 1998, pg. 306-318.

[4] R.J. Anderson, F.A.P. Petitcolas, "On the Limits of Steganography", *IEEE Journal of Selected Areas in Communications*, May, 1998, pg 474-481.

[5] Deepak Sharma, "Digital Watermarking Vs Steganography: Key Issues", Center for Advanced Computer Studies", *University of Louisiana at Lafayette*, Spring, 2003.

[6] Eric cole, "Chapter 21 Convert Communication: Goal of Digital Watermarking", *Network Security Bible, 2nd Edition*, September, 08, 2009, pg. 676.

[7] Vidysagar Potdar Elizabeth Chang, "Visibly Invisible: Cipertext as a Steganographic Carrier*", 4th International Network Conference INC 2004*, July 6th – 9th, Plymouth U.K.

[8] Mauro Barni, "Digital Watermarking", *4th International Workshop*, Siena, Italy, IWDW 2005.

[9] George Bibis, "Advances in Visual Computing", *4th International symposium*, Las, ISVC, 2008.

[10] Eric Cole, Ronald d. Krutz, "Hiding in Plain Sight: Steganography and the Art of Convert Communication", *Bob Ipsen*, 2003, WilePublishing Ltd.

[11] T. Furon and P. Duhamel, "An Asymmetric Watermarking Method", *IEEE Transaction on Signal Processing*, April 2003, Vol, 51, No.4.

[12] Wojciech Fraczek, Wojciech Mazurczyk, Krzysztof Szczypiorski, "Multi-Level Steganography: Improving Hidden Communication in Networks", *Warsaw University of Technology*.

[13] S. Radharani Dr. M.L. Valarmathi, "A Study on Watermarking Schemes for Image Authemtication", *International Journal of Computer Applications* (0975-8887), May, 2010, Vol 2, No. 4.

[14] http://ebookbrowse.com/chapter-13-steganography-and-watermarking-ppt-d144708320#.

[15] Neil F. Johnson, Zoran Duric, Sushil Jajodia, "Information Hiding: Steganography and Watermarking: attacks and countermeasures", *Springer*, 2001.

[16] Ingemar J. Cox, Matthew Miller, Jeffrey Bloom, "Digital Watermarking", *Morgan Kaufmann*, 2002.

[17] Nicholas J. Hopper John Langford Luis von Ahn, "Provably Secure Steganography", September, 2002, *CMU-CS*-02-149.

[18] C.-T. Li and F.M. Yang. One-dimensional Neighborhood Forming Strategy for Fragile Watermarking. In *Journal of Electronic Imaging*, vol. 12, no. 2, pp. 284-291, 2003.

[19] C. Podilchuk and W. Zeng. Image-adaptive Watermarking Using Visual Models. In *IEEE Journal Selected. Areas of Communications*, vol. 16, pp. 525-539, May 1998.

ISSN: 2278 – 7798

[20] C. Podilchuk and E. Delp. Digital Watermarking Algorithms and Applications. *In IEEE Signal Processing Magazine, vol. 18, no. 4*, July 2001.
[21] I. J. Cox, M.L. Miller and J.A. Bloom. Digital Watermarking. *Morgan Kaufmann, San Francisco*, USA, 2002.
[22] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," *IEEE J. Select. Areas Commun*., vol. 13, pp. 1495–1504,Oct. 1995.
[23] F. M. Boland, J. J. K. Ó Ruanaidh, and W. J. Dowling,"Watermarking digital images for copyright protection," in *Proc. Int.Conf. Image Processing and Its Applications, vol. 410*, Edinburgh,U.K., July 1995.
[24] L. Boney, A. H. Tewfik, and K. H. Hamdy, "Digital watermarks for audio signals," in *Proc. EUSIPCO* 1996, Trieste, Italy, Sept. 1996.
[25] F. Hartung and B. Girod, "Digital watermarking of raw and compressed video," in *Proc. SPIE Digital Compression Technologies and Systems for Video Commun.*, vol. 2952, Oct. 1996, pp. 205–213.
[26] William Stallings "Network Security Essentials (Applications and Standards)", *Pearson Education*, 2004.
[27] B.Schneier, Practical Cryptography,*Wiley*, 2003.
[28] National Bureau of Standards, " Data Encryption Standard," *FIPS Publication* 46, 1977.
[29] D. Salama, A. Elminaam and etal, "Evaluating The Performance of Symmetric Encryption Algorithms", *International Journal of Network Security*, Vo1.10, No.3, PP.216-222, May2010.
[30] Ramesh G, Umarani. R, " UR5:A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation", *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4*, April 2012 Page 16-22. 2010.
[31] S. Contini, R.L. Rivest, M.J.B. Robshaw and Y.L. Yin. "The Security of the RC6 Block Cipher. Version 1.0 ". August 20, 1998.
[32] Ramesh, G. Umarani, R. ,UMARAM: A novel fast encryption algorithm for data security in local area network *http://ieeexplore.ieee.org /xpl/ freeabs_all.jsp? arnumber=5670740*

Bhumi Patel*, post graduate student, Instrumentation and control engineering department, L D college of engineering, Gujarat technological university, Ahmedabad, Gujarat, India. Mobile No-9925954566*

Rakesh C Patel*, Professor, Instrumentation and control engineering department, L D college of engineering, Gujarat technological university, ,Ahmedabad, Gujarat, India*

ISSN: 2278 – 7798

Table-1 difference between cryptography and watermarking for various criteria

Criteria	Cryptography	Watermarking
Goal	The main goal of cryptography is to hide a message in some (cover) data, to obtain new data, practically indistinguishable from original data, by people, in such a way that an eavesdropper cannot detect the presence of message in new data. It is also often said that the goal of cryptography is to hide a message in one-to-one communications. [1,2,3]	The main goal of watermarking is to hide a message in some (cover) data, to obtain new data, practically indistinguishable from original data, by people, in such a way that an eavesdropper cannot remove or replace watermark in new data. The goal of watermarking is to hide message in one-to-many communications.[4,5,6]
Carrier	Any media – text file, audio, video etc.[7]	Mostly paper, image & audio.[8,9]
Secrete data	Key – embedded with carrier without knowing its presence.[10]	Watermark - embedded with carrier with or without knowing its presence.[11]
Objective	Secret communication.[12]	Copyright, authentication etc.[13]
Different methods [14,15]	**Substitution techniques** substitute redundant part of the cover-object with a secret message. **Transform domain techniques** embed secret message in a transform space of the signal (e.g. in the frequency domain). **Spread spectrum techniques** embed secret messages adopting ideas from spread spectrum communications. **Statistical techniques** embed messages by changing some statistical properties of the cover-objects and use hypothesis-testing methods in the extraction process. **Distortion techniques** store secret messages by signal distortion and measure the deviation from the original cover in the extraction step. **Cover generation techniques** do not embed messages in randomly chosen cover-objects, but create covers that fit a message that need to be hidden.	**Private (non-blind) watermarking** systems require for extraction/detection the original cover-data. **Type I systems** use the original cover-data to extract the watermark from stego-data and use original cover-data to determine where the watermark is. **Type II systems** require a copy of the embedded watermark for extraction and just yield a yes/no answer to the question weather stego-data contains a watermark. **Semi-private (semi-blind) watermarking** does not use the original cover-data for detection, but tries to answer the same question. (Potential application of blind and semi-blind watermarking is for evidence in court ownership) **Public (blind) watermarking** - neither cover-data nor embedded watermarks are required for extraction - this is the most challenging problem.
Visibility	Invisible[15]	Mostly visible[16]
Target audience	Cryptography is usually involved between very limited amount of people, only two in many cases.[17]	Watermarked products can be distributed freely among large groups of people.[17]
Attack method	Steganalysis	Data processing
Fail condition	Detection	Removal
Result	Stego-file	Watermarked file

ISSN: 2278 – 7798