Evaluation of Watermarking Techniques

Dr. A. S.N.Chakravarthy[#1],
Professor
ECM Department
K L University
A.P., India.

Prof.S.BALAJI [*2],
Professor
ECM Department
K L University
A.P., India.

Rammohanarao Koduri [#3]
Research Scholar
ECM Department
K L University
A.P.,India.

***Abstract*—Now a days the copyright of multimedia and secrete information is very difficult to transfer across the internet multimedia objects must be compressed before transmitting the data. The JPEG compression is one of the most important criteria in watermarking issue. Watermarking, which belong to the information hiding technique? There is a lot of work begin conducted in different branches in this field, Stegnography is used for secret communication, whereas watermarking is used for content protection, copyright management, content authentication and tamper detection. We classify the techniques based on different domains in which data is embedded. Here we limit the survey to images only. However, making digital data accessible to others through networks also creates opportunities for malicious parties to make sailable copies of copyrighted content without permission of the content owner. Digital watermarking techniques have been proposed as a solution to the problem of copyright protection of multimedia data in network environments.**

Keywords— Watermarking, Chinese reminder theorem, singular value decomposition, Aryabhata reminder theorem, Pell's equation.

I. INTRODUCTION

Multimedia production and distribution, as we see it today, is all digital form the authoring tools of con-tent providers to the receivers. The advantages of digital process and distribution like noise-free transmission, software instead of hardware processing, and improved reconfigurability of systems, are all well known and obvious. Not so obvious are the disadvantages of digital media distribution Watermarks designed for copyright protection, fingerprinting, or access control must also be embedded in a secure form. This means that an attacker who knows all details of the embedding algorithm except the secret key should not be able to interrupt the watermark clear of detection. Another important attribute of watermarking is the computational complexity of the embedding and extracting process. In some applications, it is important that the embedding process be as fast and simple as possible (watermarking images in digital cameras for tamper detection) while the extraction can be more time consuming. In other applications, the speed of extraction is absolutely crucial (e.g., extracting captions from digital video). Digital watermark is a perceptually see-through pattern inserted in an image using an embedding algorithm and a secret key. The purpose of the watermark is to supply some additional information about the image to identify the image owner or a particular customer, to verify image integrity, or to achieve control over the copy process of a particular digital media.

The information carried by the watermark can be can be accessed using a detection algorithm provided the secret key is known. An important property of a watermark is its robustness with respect to image distortions. This means that the watermark should be readable from images that underwent common image processing operations, such as filtering, lossy compression, noise adding, histogram manipulation, and various geometrical transformations

II. DIGITAL WATERMARKING TECHNIQUE

The process of embedding a watermark in a multimedia object l is termed as watermarking [7]. Watermark can be considered as a kind of a signature that reveals the owner of the multimedia object. Content providers want to embed watermarks in their multimedia objects (digital content) for several reasons like copyright protection, content authentication, tamper detection etc. A watermarking algorithm embeds a visible or invisible watermark in a given multimedia object. The embedding process is guided by use of a secret key which decided the locations within the multimedia object (image) where the watermark would be embedded. Once the watermark is embedded it can experience several attacks because the multimedia object can be digitally processed. The attacks can be unintentional (in case of images, low pass filtering or gamma correction or compression) or intentional (like cropping). Hence the watermark has to be very robust against all these possible attacks. When the owner wants to check the watermarks in the possibly attacked and distorted multimedia object, s/he relies on the secret key that was used to embed the watermark. Using the secret key, the embedded watermark sequence can be extracted. This extracted watermark may or may not resemble the original watermark because the object might have been attacked. Hence to validate the existence of watermark, either the original object is used to compare and find out the watermark signal (non-blind watermarking) or a correlation measure is used to detect the strength of the watermark signal from the extracted watermark (blind watermarking). In the correlation based detection the original watermark sequence is compared with the extracted watermark sequence and a statistical correlation test is used to determine the existence of the watermark.

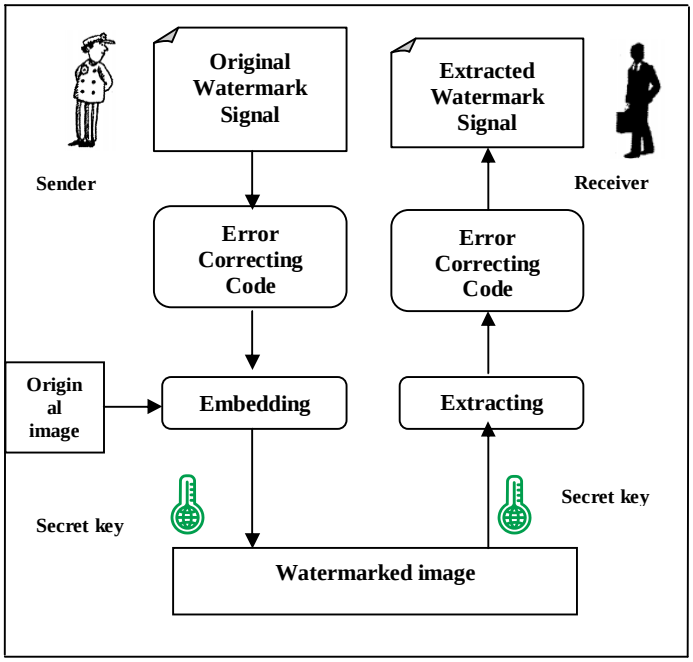

Fig.1 Watermarking Technique

In Section 3, we describe a methodology for comparing watermarking schemes.

III. COMPARISON METHODOLOGY

Most watermarking schemes contain one or more parameters that directly influence the watermark strength or visibility. In order to compare robustness of schemes in a fair manner, the parameter(s) for each scheme should be adjusted so that watermarks of approximately the same visibility (strength) are produced. The mean square error or energy of the watermark does not have to necessarily correlate with human perception. This is why we propose to use a better model of the human visual perception for watermark visibility evaluation. The PELL's equation is an arbitrary quadratic Diophantine equation with two unknowns can be reduced to a Pell-type equation. The model is even more general and can be applied to videos. In this paper, we use only the spatial portion of the model and neglect the temporal part. Some watermarking schemes are naturally formulated for embedding only one bit, while others easily accommodate multiple bits. In this paper, we present a method for converting a multiple-bit technique into a one-bit technique, and for converting techniques that embed a single bit using a spread spectrum principle into a technique that can handle multiple bits. Details of the procedures will become clear in the next Section 3 when we apply them to three watermarking techniques.

The guidelines for comparing watermarking techniques [1] are as follows:

- Adjust watermark strength so that Girod's model indicates less than α % of pixels with visible changes (α =1).
- Modify the scheme so that a one-bit watermark and a 60-bit watermark can be embedded.
- Set decision thresholds so that the probability of false detections is less than (10–6).

Repeat the experiments for all test images

IV. COMPARING THREE WATERMARKING TECHNIQUES

We chose three techniques that embed the watermark by modulating the DCT coefficients. To the best of our knowledge, these three techniques have the most impressive robustness properties. The first technique has been described as CHINESE REMINDER THEOREM. The second technique is ARYABHATA REMINDER THEOREM. A and the third one is PELL's EQUATION. The watermark strength is further adjusted according to a perceptual mask.

A. Chinese Remainder Theorem (CRT)

Chinese Remainder Theorem (CRT) is a statement about simultaneous congruencies. It is used in areas like authentication of images [2], one-way hash functions [3] and multiple description coding [4].

The SVD-based watermarking scheme proposed by Chang et al. [5] uses a block-based SVD methodology. The scheme is quite promising. However, the main weakness of this scheme is its reliance on the use of rank in selecting the image blocks for embedding watermark bits. This reliance causes the scheme to be less resistant to attacks, which alters the rank of the image blocks. In this scheme, the selection of image blocks based on higher ranks would lower the distortion level of the watermarked image. However, the rank is not a reliable feature as it is not stable. The rank could change after the modifications to coefficients 1c and 2c. Therefore, without any tampering to the watermarked image, the extracted watermark could be corrupted due to a change in rank of the block. Figure 1 shows the corruption of the extracted watermark due to changes in rank. In general, when the strength factor increases, the likelihood of changing of the rank of a block increases. This leads to a higher level of corruption and distortion of the watermark and watermarked image respectively.

B. Aryabhata REMINDER THEOREM (ART)

Consider an algorithm of Aryabhata # found in the text Aryabhata [8], which solves the linear indeterminate equation, $a \cdot x + c = b \cdot y$, for positive integers a, b and c (sometimes called

Diophantine equation). This algorithm also solves for X, given the pair of residues X mod mi = xi (for i = 1, 2). There is some underlying principle of simplicity in this solution, which has been found to be applicable to solving the general case of n residues in an iterative manner and requiring as few inverse operations as any we know of today and also without the necessity for a final modular reduction operation.

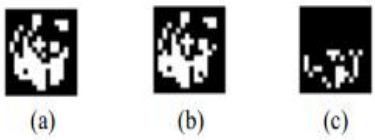

Fig.2. Watermarking Scheme 1: The change in rank results in a shifted Panda in the extracted watermark.(a) Original 16 x 16 Watermark. (b) Extracted 16 x 16 Watermarks. (c) Absolute error image [6].

This leads us to state these as Aryabhata Remainder Theorem (ART) and the ART algorithm presented here is comparable and in some ways more efficient than the CRT algorithm of Gauss, the original Garner's Algorithm [9] (and) the later version of GA.

1) Aryabhata Remainder Theorem (ART) [9]

Let m1 and m2 be relatively prime moduli and M = m1m2.

Given X mod m1 = x1, X mod m2 = x2,

X has a unique solution in ZM given by:
X = ART (x1, x2; m1, m2; M)
= ART (0, c; m1, m2; M) + x1
Where c = (x2 –x1)
modm2 = A + x1, where A = m1 [(c · m1 -1) mod m2].

Proof: First we show that X = A + x1 □ ZM.
Since A = m1 · b for some b □ Zm2,
A must be less than or equal To m1 (m2-1).Since x1 < m1,
A + x1 must be less than
M = M1m2 and therefore X □ ZM.
Now consider (A + x1) mod m1.
Since A is a multiple of m1,
We have (A + x1) mod m1 = x1.
Since A mod m2 = c due to the cancellation of
The terms m1 and m1 -1,
We have (A + x1) mod m2 = c + x1= x2.
Thus A + x1 = X satisfies the two congruence's as required and is a solution in ZM.
It is easy to show that A + x1 is a unique solution in ZM.
If Y □ ZM is another solution,
Then (X - Y) mod mi = 0, for i = 1, 2 and (X - Y) mod M = 0.
Thus X = Y.

C. PELL's EQUATION (PE)

1) Pell's equation based crypto system:

In number theory, for any constant integer D the equation x2 −Dy2 ≡ 1 is called the Pell' equation. This has many applications [10, 11] in various branches of science. The set of all pairs(x, y) describes a cyclic group called Gp over the pall's equation x2 −Dy2 ≡ 1 (mod P), where P is an odd prime. The properties of Gp are also found in the group GN over the pell's equation x2−D y2 ≡ 1 (mod N), where N is a product of two primes. This group GN then developed to be a public key crypto scheme based on Pell's equations over the ring ZN.

From the group GN, we find a group isomorphism mapping f: GN → ZN
Such that,
A solution (x, y) of the Pell's equation x2 −D y2 ≡ 1(mod N), can easily be transformed to unique element u in ZN*.This implies that the plain texts/cipher texts in the group GN can be transformed to the corresponding plain texts/cipher texts like in the RSA scheme. Let p be an odd prime and D be a non zero quadratic residue element modulo p, which we denote if with Fp.
Gp denotes the set of solutions (x, y) □ Fp* Fp to the pell's equation x2− D y2 ≡ 1 (mod P).

We then define an addition operation " $\oplus$ "on Gp as follows.

If two pairs (1x, 1y), (2x ,2y) $\oplus$ Gp, then
The third pair (3x , 3y) can be computed as
(3x ,3y) $\oplus$ (1x ,1y) $\oplus$(2x ,2y) $\oplus$ (1x2x +D1y2y ,1x2y +2x1y) (mod p) .

It is easy to verify that the Gp together with the operation" $\oplus$ " is an abelian group with the identity element being (1,0) and the inverse of the element (x, y) being (x,-y). Further it can be proved that <Gp, $\oplus$ > is a cyclic group of order p-1. Now we want to prove that the group Gp is isomorphic to Fp*, where Fp*, is all non-zero elements of Fp denotes a multiplicative group of Fp.

IV.*CONCLUSION AND FUTURE DIRECTIONS*

In this paper, we presented a methodology for comparing the robustness of watermarking schemes. In order to compare the techniques in a fair manner, we propose to adjust the watermark strength so that a fixed model of the human visual system detects the same extent of artifacts (the spatial masking model of Girod3 is proposed for this purpose). Furthermore, we describe a methodology for converting a detectable, one bit watermark into a readable watermark and vice versa. Finally, the detection statistics (threshold) is adjusted so that the probability of false detections is less than 10–6. Therefore, as a conclusion, we prefer Method 3 because of better security properties and slightly better robustness.

ACKNOWLEDGMENT

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The authors would like to thank K.L. University management for providing necessary facilities to carry out this work

REFERENCES

[1] Jiri Fridrich* a,b, Miroslay Goljan Center for Intelligent Systems, SUNNY Binghamton, Binghamton, NY 13902-6000, Mission Research corporation, 1720 Randolph Rd SE, Albuquerque, NM 87106.

[2] Y. Yang, F. Bao and R.H. Deng, "Flexible authentication of images", in Proc. of the SPIE, Visual Communications and Image Processing 2003.Edited by Ebrahimi, Touradj; Sikora, Thomas. vol. 5150, pp. 1905-1911, 2003.

[3] M.S. Hwang, C.C. Chang, and K.F. Hwang, "A watermarking technique based on one-way hash functions", IEEE Transactions on Consumer Electronics, vol. 45, no. 2, pp. 286-294, May 1999.

[4] C. Candan, "A multiple description coding scheme based on the Chinese remainder theorem", in Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 4, May 2002, pp. IV-3525 – IV-3528.

[5] C.C. Chang, P. Tsai and C.C. Lin, "SVD-based digital image watermarking scheme", Pattern Recognition Letters, vol. 26, pp. 1577-1586, 2005.

[6] C. Bornand HEIG-VD, Yverdon-les-Bains University of Applied Sciences, Switzerland 2008 IEEE International Conference on Systems, Ma n and Cybern etics (SMC 2008)

[7] Vidyasagar M. Potdar, Song Han, Elizabeth Chang School of Information Systems, Curtin University of Technology, Perth, Western Australiahttp://www.petitcolas.net/fabien/watermarking/stinnark

[8] Cryptography and Information SecurityMaiko Kobe, Japan, Jan. 25-28, 2005 The Institute of Electronics,Information and Communication Engineers

[9] H. Garner, "The residue number system", IRE Transactions on Electronic Computers, EC-8, pp. 140–147, 1959.

[10] Chiou, C.W and Yang, T.C. (1994):" Iterative Modular Multiplication algorithm without Magnitude Comparison," Electronic letters. Vol. 30, No. 24, Nov. 94, pp 2017-2018.

[11] Hasted, j. (1985):"On Using RSA with low exponent in a public key Network," Proc. Of CRYPTO-85, Springer-verlag, New York, 1986, pp. 403-408.

AUTHORS PR0FILE

Dr. A. S .N. Chakravarthy, currently is working as Professor in Dept. of Electronics and Computer Engineering in K.L. University, Guntur. He has 21 papers published in various International journals and conferences. His research areas include Cryptography, Biometrics, and Digital Forensics. He is Reviewer and Editorial board member for various International Journals.

Prof. S. Balaji, currently working as HOD & Professor in Dept. of Electronics and Computer Engineering in K.L. University, Guntur. He has published 21 Papers in various National / International journals and conferences. His Research Areas are Image Processing, Biometrics and security.

K.Rammohanarao, currently pursuing M.Tech Degree in the Department of Electronics & Computer Engineering in K.L.University, Guntur.