Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks

Dr. Swati Sherekar
SGB Amravati University
ss_sherekar@rediffmail.com

Dr. V.M.Thakare
SGB Amravati University
vilthakare@yahoo.co.in

Dr. Sanjeev Jain
SATI ,Vidisha (M.P.)
dr_sanjeevjain@hotmail.com

ABSTRACT

Robustness against attacks is a major watermarking requirement. Absolute robustness against all possible attacks and their combinations may be impossible to achieve.

In this paper, investigation made regarding the various attacks on the digital watermarking systems and its categorization. Attacks on digital watermarks must consider both watermark survival and the distortion of the attacked document. Theoretical analysis of watermark attacks gives many insights into the watermarking problem. Therefore, the paper is concluded with the practical implications of watermarking benchmarks and countermeasures. In fact, with appropriate design, fairly high robustness can be achieved, but it should be pointed out that robustness always has to be traded against watermark data rate and imperceptibility, and the optimum tradeoff depends on the application.

Keywords:- digital watermark, benchmark, copyright protection, attacks, robustness.

5. INTRODUCTION

In the world of internet, multimedia communication becomes very easy, efficient and cost effective. Digital multimedia can be easily tampered and manipulated. Digital watermarks have been proposed as a means for copyright protection for multimedia data. Various watermarking schemes are designed mainly for copyright protection and data authentication. In case of copyright protection, the identification of an image's rightful owner is important. The embedded information should be decodable from the watermarked data, even if the watermarked data is processed, copied, or redistributed.[1] Potential applications of digital watermarking include copyright protection, distribution tracing, authentication, authorized access control as well as covert communication.

6. WATERMARKING TECHNIQUE

The watermark is an additive signal w, which contains the encoded and modulated watermark message under constraints given by a mask *M* so that I' = *x* + *w(M).*

Note that w need not be independent from the original data x. The simplest approach to achieve a perceptually indistinguishable watermarked and original signal is to keep the power of the watermark signal very low. Using sophisticated psycho-acoustic or psycho-visual models, more appropriate masks *M* can be applied to enhance the robustness of the watermarking scheme.

The media used for watermarking can be broadly classified into text, image, audio and video. Two domains are used for processing various methods spatial domain and frequency domain.[2,3] Commonly used embedding techniques can be classified into additive, multiplicative, and quantization-based schemes.

The term watermark itself is not always well- defined in the literature. To be precise, there must be clear cut discrimination between the watermark signal *w,* which is the actual signal added to the original data, and the watermark message or information *b* that is conveyed by the watermark signal. Usually the meaning is clear from context. Coding schemes can be used to achieve reliable watermark communication.

Based on robustness, watermarking scheme can be divided into fragile, semi-fragile and robust.[4] Robustness is the capacity of tolerance of attacks on the watermarked data.

In watermarking technology, any processing that may impair the detection of the watermark is called as attack.[5] In addition to the counterfeit attacks introduced in this paper, study of watermarking schemes that are robust against general attacks to remove or diminish the presence of the watermark in the watermarked images is elaborated.

These attacks easily allow any one to claim ownership of any images one who access to, whether those images have been watermarked or not. The unfortunate fact is that unwatermarked images will fall prey to false ownership claims by someone exploiting the attacks. How to protect these unwatermarked images against deliberate attacks is an issue worthy of further research. In spite of the promises of digital watermarking, one has to select carefully the watermarking scheme based on the application.

7. WATERMARKING ATTACKS

In most watermarking applications, the marked data is likely to be processed in some way before it reaches the watermark receiver. The processing could be lossy compression, signal enhancement, or digital-to-analog (D/A) and analog-to-digital (A/D) conversion. An embedded watermark may unintentionally or inadvertently be impaired by such processing. Other types of processing may be applied with the explicit goal of hindering watermark reception. In watermarking terminology, an *attack* is any processing that may impair detection of the watermark or communication of the information conveyed by the watermark. The processed watermarked data is then called *attacked data*.[5,6]

An important aspect of any Watermarking scheme is its robustness against attacks. The notion of robustness is intuitively clear. A watermark is robust if it cannot be impaired after rendering the attack on the data. Watermark impairment can be measured by criteria such as miss probability, probability of bit error, or channel capacity. For multimedia, the usefulness of the attacked data can be gauged by considering its perceptual quality or distortion. Hence, robustness can be evaluated by simultaneously considering watermark impairment and the distortion of the attacked data. An attack succeeds in defeating a watermarking scheme if it impairs the watermark beyond acceptable limits while maintaining the perceptual quality of the attacked data. Since the complete theoretical analysis of the watermarking algorithm performance with respect to different attacks is rather complicated, the developers of watermarking algorithms refer to the results of experimental testing performed in the scope of some benchmark. The benchmark combines the possible attacks into a common framework and weights the resulted performances depending on the possible application of the watermarking technology.

Early attacks do not exploit as much knowledge of the watermarking scheme as possible; also, they do not consider the distortion of the attacked document. Since attacks can be improved by using knowledge of the watermarking scheme and the signal statistics.[7] The watermarking and attacking problem is instance between the embedder and attacker can be exploited to find the watermark capacity, while facing an optimized attack with a constrained attack distortion.

8. WATERMARKING ATTACKS CLASSIFICATION

Categorization of the wide class of existing attacks contains many classes or attacks: e.g. removal attacks, geometric attacks, cryptographic attacks, and protocol attacks etc. Here, we describe coarsely these attacks types.

8.1 Active attacks:

Here, the hacker tries deliberately to remove the watermark or simply make it undetectable.[7,8] This is a big issue in copyright protection, fingerprinting or copy control.

8.2 Passive attacks:

In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not.[9] Protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one want to grant.

8.3 Collusion attacks:

In collusive attacks, the goal of the hacker is the same as for the active attacks but the method is slightly different.[10] In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, each signed with a key, to construct a new copy without any watermark. This is a problem in fingerprinting applications *(e.g.* In the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that number is pretty important.

8.4 Forgery attacks:

This is probably the main concern in data authentication.[11] In forgery attacks, the hacker aims at embedding a new, valid watermark rather than removing one. By doing so, it allows one to modify the protected data and then, re-implants a new given key to replace the destructed (fragile) one, thus making the corrupted image seems genuine.

8.5 Simple attacks:

(other possible names include “waveform attacks” and “noise attacks”) are conceptually simple attacks that attempt to impair the embedded watermark by manipulations of the whole watermarked data [9,12] (host data plus watermark) without an attempt to identify and isolate the watermark. Examples include linear and general nonlinear filtering, waveform-based compression (JPEG, MPEG), addition of noise, addition of an offset, cropping, quantization in the pixel domain, conversion to analog, and gamma correction.

8.6 Detection-disabling attacks:

(other possible names include “synchronization attacks”) are attacks that attempt to break the correlation and to make the recovery of the watermark impossible or infeasible for a watermark detector,[13] mostly by geometric distortion like zooming, shift in spatial or temporal (for video) direction, rotation, shear, cropping, pixel permutations, subsampling, removal or insertion of pixels or pixel clusters, or any other geometric transformation of the data.

8.7 Ambiguity attacks:

(other possible names include “deadlock attacks,” “inversion attacks,” “fake watermark attacks,” and “fake-original attacks”) are attacks that attempt to confuse by producing fake original data or fake watermarked data.[14] An example is an inversion attack that attempts to discredit the authority of the watermark by embedding one or several additional watermarks such that it is unclear which was the first authoritative watermark.

8.8 Removal attacks:

Removal attacks are attacks that attempt to analyze the watermarked data, estimate the watermark or the host data, separate the watermarked data into host data and watermark, and discard only the watermark. Removal attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm[15] (e.g., without the key used for watermark embedding). That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data. This category includes denoising, quantization (e.g., for compression), remodulation, and collusion attacks. Not all of these methods always come close to their goal of complete watermark removal, but they may never the less damage the watermark information significantly. Sophisticated removal attacks try to optimize operations like denioising or quantization to impair the embedded watermark as much as possible while keeping the quality of the attacked document high enough. Usually, statistical models for the watermark and the original data are exploited within the optimization process.

8.9 Cryptographic attacks:

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks.[16] One such technique is brute-force search for the embedded secret information. Another attack in this category is the so-called Oracle attack, which can be used to create a non-watermarked signal when a watermark detector device is available. Practically, application of these attacks is restricted due to their high computational complexity.

8.10 Protocol attacks:

Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of *invertible watermarks***.** The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data.[15,17] This can create ambiguity with respect to the true ownership of the data. It has been shown that for copyright protection applications, watermarks need to be noninvertible. The requirement of non invertibility of the watermarking technology implies that it should not be possible to extract a watermark from a non-watermarked document. A solution to this problem might be to make watermarks signal-dependent by using one-way functions.

8.11 Copy attacks:

Another protocol attack is the *copy attack.* In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called *target data.*[18] The estimated watermark is adapted to the local features of the target data to satisfy its imperceptibility. The copy attack is applicable when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor knowledge of the watermarking key. Again signal-dependent watermarks might be resistant to the copy attack or different watermark, can be obtained by an attacker or a group of attackers. In such a case, a successful attack can be achieved by averaging all copies or taking only small parts from each different copy. Recent results show that a small number of different copies (e.g., about 10) in the hands of one attacker can lead to successful watermark removal.

8.12 Geometric attacks:

In contrast to removal attacks, *geometric attacks* do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information.[17,19] The detector could recover the embedded watermark information when perfect synchronization is regained. However, the complexity of the required synchronization process might be too great to be practical.

8.13 Estimation-based attacks

In this type of attacks, the knowledge of watermarking technology is consider and exploit statistics of the original data and watermark signal. [15,20] This concept is based on the assumption that the original data or the watermark can be estimated - at least partially from the watermarked data using some prior knowledge of the signals' statistics. Note that estimation does not require any knowledge of the key used for watermark embedding. Further more, knowledge of the embedding rule is not required, but the attack can be more successful with it. Depending on the final purpose of the attack, the attacker can obtain an estimate of the original data or of the watermark based on some stochastic criteria such as maximum likelihood (ML), maximum a posteriori probability (MAP), or minimum mean square error (MMSE).

9. RECENT TRENT IN ATTACKS

In this section, as per recent trends and technology, attacks on digital watermarking are discussed. [32,33]

H. T. Sencar et. al. [31] proposed embedding multiple watermarks and detecting a randomly selected subset of them while constraining the embedding distortion. Problem common to most watermarking-based ownership is that, dispute resolutions and ownership assertion systems.

The bottom line of the scheme lies in both watermark generation, which deploys a family of one-way functions and selective detection, which injects uncertainty into the detection process. The potential of this approach is in reducing the false-positive probability under various operating conditions and compared to single watermark embedding. The multiple watermark embedding and selective detection technique is implemented into the additive watermarking technique and results proves effectiveness through numerical solutions.

Thanh-Ha Le et. al.[34] proposed a new method to reduce the Gaussian noise of signals in DPA and CPA attacks using the fourth-order cumulant of side channel signals.[35] Side channel attacks exploit physical information leaked during the operation of a cryptographic device (e.g., a smart card). The confidential data, which can be leaked from side channels, are timing of operations, power consumption, and electromagnetic emanation. The evaluation based on two criteria- the probability of detection and the SNR with flexible parameters, such as the noise level, the number of side channel signals, and the length of sliding window. This preprocessing method based on the fourth-order cumulant, which improves the performance of side channel attacks. The cumulant method is a powerful solution for the noise suppression and the temporal misalignment correction in a side channel attack.

Daniel S. Fava et. al. [36] introduces a framework for the characterization and prediction of cyberattack behavior. This approach aims at capturing the sequential properties residing in the correlated IDS alerts as per existing technologies, namely, IDSs and alert correlation engines which does not require the modeling of network configuration and system vulnerabilities. The behavior trends exhibited in various fields of IDS alerts are captured via VLMMs. Results demonstrate that sequential properties (i.e., the first-, second-, third-, order Markov models are all beneficial and a combination of them via VLMM leads to the best prediction accuracy). Information theory-based metrics, such as entropy and log loss, are proposed as indicators of the prediction quality.

The battle against cyber attacks goes beyond password protection, encryption, intrusion detection, and alert correlation. Having these components is essential for protected network operations and usage; however, a proactive measure that projects ongoing attack actions is crucial for timely mitigation of cyber attack impacts. In order to create a comprehensive assessment of cyber attacks, this presented approach to be considered as part of the cyberattack projection solution, complementing the projection schemes that depend on network-specific information.

X. Wang et.al. [37] proposes a novel feature-based image watermarking scheme against desynchronization attacks is proposed, which can survive various signal processing and affine transformation and are extracted by using the Harris–Laplace detector.[40] A local characteristic region (LCR) construction method based on the scale-space representation of an image is considered for watermarking. At each LCR, the digital watermark is repeatedly embedded by modulating the magnitudes of discrete Fourier transform coefficients. In watermark detection, the digital watermark can be recovered by maximum membership criterion.

Simulation results show that the proposed scheme is invisible and robust against common signal processing, such as median filtering, sharpening, noise adding, JPEG compression, etc., and desynchronization attacks, such as rotation, scaling, translation, row or column removal, cropping, and random bend attack.

M. El Choubassi et.al [41] presents a framework to design randomized detectors with exponentially large randomization space and controllable loss in detection reliability and also devise a general procedure to attack the detectors by reducing them into equivalent deterministic detectors. Spread spectrum schemes are vulnerable against sensitivity analysis attacks on standard deterministic watermark detectors. A proper randomized watermark detector should be use against it. While randomization sacrifices some detection performance, it might be expected to improve detector security to some extent.

Randomization of the detector is not the ultimate answer for providing security against sensitivity analysis attacks in spread spectrum systems since the randomized detector inherits the weaknesses of the equivalent deterministic detector.

D. Gafurov et. al. [42] focus on a new biometric technique used for spoof attacks. Biometrics, such as voice, handwritten signature, keystroke dynamics reported promising results. Research in biometric gait recognition has increased now a days and gait can be vulnerable to impersonation attacks. This type of attack has already been investigated in the case of speaker and handwritten signature verifications. Author evaluated the performance of WS-based gait recognition in two different scenarios, namely, friendly and hostile. In the friendly scenario, using gait data set from 100 subjects and obtained the 13% EER and 73.2% recognition rate (i.e., identification probability at rank 1).

It is observed that indicate that a minimal effort impersonation attack on gait does not significantly increase the chances of impostors being accepted; in general, the minimal- effort mimicry on gait biometrics may not help. However, an attacker with knowledge of the closest match in the database can be a serious threat to the gait authentication system.

10. COUNTERMEASURES AGAINST ATTACKS

In the following section, countermeasures are given that make watermarks more robust against malicious attacks.

10.1 Countermeasures Against Simple, Waveform-Based Attacks:

As already mentioned, noise-like distortions, for example, due to lossy compression, result in a distorted watermark signal in the watermark recovery or verification process. There are two main countermeasures against such attacks: increasing the embedding strength or applying redundant embedding. Increasing the embedding strength is straightforward and efficient in many cases, especially if appropriate masking according to the properties of human perception is used to determine the maximum allowable embedding strength.[24,27] Redundant embedding can be performed in many ways. In the spatial domain it might consist of embedding a watermark many times and then taking a majority vote in the recovery process. A more efficient technique could include the use of error-correcting codes. Both increasing the watermark strength and introducing redundancy either increase the watermark visibility/audibility or decrease the watermark data rate. Further, as pointed out before, it should be noted that there is a tradeoff between watermark robustness on one hand and watermark imperceptibility and watermark data rate on the other hand.

10.2 *Geometrical Distortions and Countermeasures:*

Watermarks are typically most vulnerable to geometrical distortions. The reason is that, for most proposed watermarking methods, the watermark detector has to know the exact position of the embedded watermark. Geometrical distortions tend to destroy the synchronization such that watermark embedding and watermark detection are misaligned and do not fit anymore.[29] Simple geometric attacks include affine transforms, clipping, and cropping. Remedies against such attacks are difficult if the watermarking algorithm has not explicitly been designed to withstand such attacks. For these “simple” geometrical attacks, the challenge consists of finding the original watermark reference within the host data. For watermarking schemes which require the original image to recover the watermark this may not be a real problem, since the geometrical distortion can be estimated from the two images and inverted.[22,26] If the watermarking scheme does not have the original data available for the watermark recovery, many schemes still allow the reference recovery by using a full search over all possible manipulations using some kind of correlation criteria between the image and the watermark modulation sequence. If the geometrical distortion consists of simple cropping, translation, or rotation, this process is feasible. However, if the attack consists of any affine transform this becomes very intensive computationally.

10.3 Watermark Removal Attacks and Countermeasures:

Collusion attacks are attacks that use several copies of the same host data with different embedded watermarks. Several types of collusion attacks have been examined by Cox and Stone. In the following, a watermark observation refers to a watermarked data representation in any domain, e.g., spatial or frequency domain. The first attack is called statistical averaging, in which a new data set is created by taking the average of all available watermark observations.[25] A second attack creates a new data set by taking the average of the minimum and maximum of all watermark observations.[28] In general, all these statistical attacks can successfully destroy embedded watermarks even if only a few watermarked data sets are available. Another collusion attack interleaves the different watermarked copies of the same data. Small parts of different watermarked data sets are taken and reassembled in a new data set. A countermeasure against collusion attacks is to limit the available number of watermarked copies. Alternatively, it has been proposed to use collusion-secure codes to design watermarks. The drawback is that the code lengths increase exponentially with the number of codes.

10.4 Countermeasures against Active Attacks:

If the attacker first removes the mark from the image then the image is modified and finally the mark is embedded again then in these cases the content-based or invertible watermarking algorithm is effective to resist the attack.[21]

10.5 Countermeasures against Estimation-based Attacks:

Attacker can modify the marked image based on some prior knowledge of the signals' statistics, without affecting the embedded mark. For example, in quantization based watermarking algorithm, the value of the extracted watermark is determined by the quantization interval of marked image coefficients. If the attacker knows this quantization interval he can easily modify the image coefficients without changing the extracted watermark.[15]To solve the situation HVS model can be used to have better solution.

10.6 Countermeasures against Noise or Simple Attacks:

The attacker may attempt to completely destroy the mark by adding random noise, which is the most common type of attack.[23] Improvement in the robustness of semi-fragile watermark is the only countermeasure, but if the attacker adds excessive noise, image quality degraded totally.

11. BENCHMARKING

The results of experimental testing performed in the scope of some benchmark. The developers of watermarking algorithms need the tool for the analysis and performance of the watermarking algorithm with respect to different attacks. [7,30]

The benchmarking initiatives for image watermarking schemes can be elaborated through various benchmarking tools used for watermarking.

11.1 Stirmark:

Stirmark has been developed by Fabien Petitcolas at Cambridge University, UK. Since its first publication in 1997, Stirmark has gained large interest from the watermarking community and it is currently the most widely used benchmarking suite for digital watermarking technologies. The Stirmark benchmark divides attacks into the following nine categories: signal enhancement, compression, scaling, cropping, shearing, rotation, linear transformations, other geometric transformations, and random geometric distortions. In the case of signal scaling, cropping, shearing, rotation, linear transformations, and other geometric transformations, the attacked images are obtained with and without JPEG 90 percent quality factor compression. In order to produce a score relative to the benchmark, **a** score of **1** is assigned when the watermark is decoded and 0 when it is not decoded. The average is then computed for each category, and the average of the results is computed to obtain an overall score. The benchmark should also average over several images. In order to ensure a fair comparison, Petitcolas suggests imposing a minimum PSNR of 38 dB for the watermarked image. However, this constraint is questionable since PSNR is not a meaningful measurement in the context of geometric distortions.

11.2 CERTI MARK:

CERTIMARK (Certification for watermarking techniques), European project that addresses the issue of design and development of a complete benchmark suite for watermarking technologies. Certimark is used to design, develop and publish a complete benchmark suite for still picture and video watermarking technologies within promising application scenarios, aiming at making this benchmark suite as a reference tool and to concentrate on research on the pending key issues in watermarking for protection of still images and low-bit-rate video over the Internet. CERTIMARK benchmark suite is based on modular organization, to allow for a variety of parameters and application types. Certification module: takes into account the different criteria and application typology to evaluate a watermarking system and validate it as certified for a range of applications.

The aim of Certimark, based on the benchmark reference, is to make watermarking algorithms labeled with an international certification. This certification process and award will be conducted by a major international rights holder representative. Benchmarking, leading to an internationally recognized reference, will permit customers to assess the appropriateness of a given watermarking technology for their needs. Assessment of technologies in a clear framework will allow competition between technology suppliers while maintaining a given quality standard measured by the benchmark. The Certimark, gives the emphasis on the parallel development of objective evaluation tools and robust watermarking techniques.

For image watermarking, the best known benchmarking tools, Unzign and Stirmark, integrate a variety of geometric attacks. Unzign introduces local pixel jittering and is very efficient in attacking spatial domain watermarking schemes. Stirmark introduces both global and local geometric distortions.

However, most recent watermarking methods survive these attacks due to the use of special synchronization techniques. Robustness to global geometric distortions often relies on the use of either a transform-invariant domain (Fourier- Melline) or an additional template, or specially designed periodic watermarks whose autocovariance function (ACF) allows estimation of the geometric distortions. However, as discussed below, the attacker can design dedicated attacks exploiting knowledge of the synchronization scheme. Robustness to global affine transformations is more or less a solved issue. However, resistance to the local random alterations integrated in Stirmark still remains an open problem for most commercial watermarking tools. The so called random bending attack in Stirmark exploits the fact that the human visual system (HVS) is not sensitive to local shifts and affine modifications. Therefore, pixels are locally shifted, scaled, and rotated without significant visual distortion. However, it is worth noting that some recent methods are able to resist this attack.

11.3 Checkmark:

Checkmark is a benchmarking suite for digital watermarking technologies. Running on Matlab under UNIX and Windows, it provides efficient and effective tools to evaluate and rate watermarking technologies. Checkmark contains some attacks which are not present in Stirmark. It includes new classes of tests such as Wavelet compression (jpeg 2000 based on Jasper) Projective transformations , Modeling of video distortions based on projective transformations Warping, Copy , Template removal , Denoising (midpoint, trimmed mean, soft and hard thresholding, wiener filtering) , Denoising followed by perceptual remodulation, Non-linear line removal ,Collage etc. In addition the following known test classes are re-programmed from Stirmark and included: Cropping ,Flip, Rotation, Rotation-Scale , FMLR, sharpening, Gaussian filtering, Random bending, Linear transformations , Aspect ratio, Scale changes , Line removal, Color reduction, JPEG compression

11.4 Optimark:

Optimark is a benchmarking tool for still image watermarking algorithms that was developed in the Artificial Intelligence and Information Analysis Laboratory at the Department of Informatics, Aristotle University of Thessaloniki, Greece. Its main features are as follows: Graphical user interface, Detection/decoding performance evaluation using multiple trials utilizing different watermaking keys and messages, Evaluation of the following detection performance metrics: For watermark detectors that provide a float output, i.e. the value of the test statistic used for detection. For watermark detectors that provide a binary output, i.e. a value that states whether the watermark has been detected or not: Evaluation of the following decoding performance metrics, for algorithms that allow for message encoding (multiple bit algorithms): Bit error rate, Percentage (probability) of perfectly decoded messages. Evaluation of the mean embedding and detection time. Evaluation of the algorithm payload (for multiple bit algorithms). Evaluation of the algorithm breakdown limit for a certain attack and a certain performance criterion, i.e., evaluation of the attack severity where algorithm performance exceeds (or falls below) a certain limit. Result summarization in multiple levels using a set of user defined weights on the selected attacks and images. Option for both user defined and preset benchmarking sessions. Optimark was partially supported by EU Projects CERTIMARK & INSPECT. Optimark includes the following attacks:Cropping, Line and Column Removal, General Linear Transformation, Scaling, Shearing Horizontal Flip, Rotation, Rotation and Autocropping, Rotation and Autocropping and Autoscale Sharpening, Gaussian Filtering, Median, Jpeg etc.

12. OBSERVATION AND EVALUATION

To the malicious attacks, one must add all signal processing operations involved in the transmission or storage of data, which can naturally degrade the image and alter the watermarked information to the point of not being detectable anymore. Attacks can be improved by using knowledge of the watermarking scheme and signal statistics. Analysis of watermark attacks gives many insight into the watermarking problem, enables to show fundamental limits of the technology. In fact, the identification and classification of attacks, as well as the implantation of a standard benchmark for robustness testing is of great importance and will be a key issue in the future development of watermarking.

The general idea is to estimate the watermark and exploit it to trick the detector. Conclusion can be made that watermarking and attacking problem is a tradeoff between the embedder and attacker and can be exploited to find the watermark capacity.

Whether the development of watermarking technology will become a success story or not is an interesting yet unclear question. Watermarking technology will evolve, but attacks on watermarks as well. Careful overall system design under realistic expectations is crucial for successful

applications. There is a huge demand from content providers and IPR owners.

At the end describe the benchmarking, which leads to an internationally recognized reference, will permit customers to assess the appropriateness of a given watermarking technology for their needs and able to test robustness of the watermark and image quality.

13. CONCLUSION

Robustness against attacks is a major watermarking requirement. Absolute robustness against all possible attacks and their combinations may be impossible to achieve. Thus, the practical requirement is that a successful attack must impair the host data to the point of significantly reducing its commercial value before the watermark is impaired so much that it cannot be recovered. In fact, with appropriate design, fairly high robustness can be achieved, but it should be pointed out that robustness always has to be traded against watermark data rate and imperceptibility, and the optimum tradeoff depends on the application.

14. REFERENCES

[6] A. Miyazakim and A. Okamoto, “ Analysis Of Watermarking Systems In The Frequency Domain And Its Application To Design Of Robust Watermarking Systems”, Kyushu University, Fukuoka, JAPAN, pp 506-509, IEEE 2001.

[7] S. S. Sherekar, V. M. Thakare, Sanjeev Jain, “Role of Digital Watermark in e-governance and e- commerce” , International Journal of Computer Science and Network Security”, vol 8, No. 1, pg. no. 257-261, January 2008.

[8] S. S. Sherekar, V. M. Thakare, Sanjeev Jain, “Critical Review of Perceptual Models for Data Authentication” proceedings of Int. Conf. of ICETET, pp 323-329, IEEE Computer society, Dec 09.

[9]] S. Liu, L.Yongliang and W. Gao, “Secure Watermark Detection Schemes”, IEEE Asia-pacific conf. on Communications, pp 631- 633, IEEE 2004.

[10] L. Yongliang and W. Gao, “Secure Watermark Verification Scheme”, IEEE Int. Conf. on multimedia and Expo ICME, pp 923-926, IEEE 2004.

[11] Chun-Hsiang Huang ,Ja-Ling Wu, “Attacking Visible Watermarking Schemes”, IEEE Transactions On Multimedia, Vol. 6, No. 1, February 2004.

[12] Voloshynovskiy et al.. "Attack Modeling: Towards a Second Generation Watermarking Benchmark," Sig. Processing. Special Issue on Information Theoretic Issues in Digital Watermarking, 2001, vol. 81, pp. 1177-214.

[13] L. Tong and Q.Z.Ding, “The survey of digital watermarking based image authentication techniques”, ICSP’02 proceedings, pp 1556-1559, IEEE 2002.

[14] L. Tong and Q.Z.Ding, “the survey of digital water marking based image authentication techniques”, ICSP’02 proceedings, pp 1556-1559, IEEE 2002.

[15] Bangaleea and H.C.S. Rughoopth, “Performance Improvement on Spread Spectrum Spatial Domain

Watermarking Scheme Through Diversity and Attack Characterisation", pp 293-298, IEEE Africon 2002.

[16] S. Voloshynovskiy, S. Pereira,T. Pun, J. Eggers and J. K. Su, "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks" pp 118-126,IEEE Communications Magazine August 2001.

[17] J. Du, C. H. Lee, H.K. Lee and Y. Suh, "BSS: A New Approach for Watermark Attack", published in proceeding of the Fourth International Symposium on Multimedia Software Engineering, IEEE Computer Society, 2002.

[18] H.Huang and J.L.Wu , "Attacking Visible Watermarking Schemes", IEEE Trans. on Multimedia, Vol. 6, No. 1, pp 16-30, Feb 2004.

[19] S. Craver, N. Memon, B.L. Yeo, and M. M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications" IEEE Journal on Selected Areas In Communications, Vol. 16, No. 4, pp 573-586, May 1998.

[20] W. Zeng and B. Liu, "A Statistical Watermark Detection Technique Without Using Original Images for Resolving Rightful Ownerships of Digital Images", IEEE Transactions on Image Processing, Vol. 8, No. 11, pp 1534-1548, November 1999.

[21] Dittmann,P. Wohlmacher and K.Nahrstedt, "Multimedia and Security Using Cryptographic and Watermarking Algorithms", IEEE,2001, pp 54-65, 2001.

[22] C.S.Lu, S.W.Sun, C.Y.Hsu, and P.C.Chang, "Media Hash-Dependent Image Watermarking Resilient Against Both Geometric Attacks and Estimation Attacks Based on False Positive-Oriented Detection", IEEE Transactions On Multimedia, Vol. 8, No. 4, pp 668-685, August 2006.

[23] M. Kutter, Voloshynovskiy, and A. Herrigel, "Watermark Copy Attack," IS&T/SPIE 72th Annual Symp, Electronic Imaging 2000.

[24] Licks, R.Jordan, "Geometric Attacks on Image Watermarking Systems", Survey Article, Published by the IEEE Computer Society, pp 68– 78, 2005.

[25] Voloshynovskiy,, "Generalized Watermark Attack Based on Watermark Estimation and Perceptual Remodulation, " IS& T/SPIE 12th Annual Symp., Electronic maging 2000: Security and Watermarking of Multimedia Content , pp. 358-70, 2000.

[26] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques", proc. of IEEE, vol. 87, no. 7, pg. no. 1079-1107, 1999.

[27] V. Licks, R.Jordan, "Geometric Attacks on Image Watermarking Systems", Survey Article, Published by the IEEE Computer Society, pp 68– 78, 2005.

[28] F. Hartung. J. K. Su. and B. Girod. "Spread Spectrum Watermarking: Malicious Attacks and Counter-Attacks," Security and Watermarking of Multimedia Contents, Proc. SPIE. vol. 3657, San Jose, CA, Jan. 1999.

[29] Craver et al.,"On the Invertibility of Invisible Watermarking Techniques," Proc. IEEE Int. Conf, Image Processing 1997, vol.1, pp. 540-43.

[30] W. Wong and E. J. Delp, "Security and Watermarking of Multimedia Content", Eds.SPIE Proc., vol.3971, San Jose, CA, Jan. 2000.

[31] V. Senthil, R. Bhaskaran, "Wavelet Based Digital Image Watermarking with Robustness against Geometric Attacks", Conference on Computational Intelligence and Multimedia Applications, International Conference on Volume 4, 13-15 Dec. 07 , Page(s):89-93,2007.

[32] V.M.Potdar, S.Han, Chang, "A survey of digital image watermarking techniques" Industrial Informatics, Indian'05. 2005 3rd IEEE International Conference on 10-12 Aug. 2005 Page(s):709 – 716, 2005.

[33] Lian Cai, Sidan Du, "Robust digital image watermarking method against RST attacks" Signal Processing and Communications, 2004. SPCOM '04. 2004 International Conference on
11-14 Dec. 2004 Page(s):491 – 495, 2004.

[35] E. Mwangi, "A Geometric Attack Resistant Image Watermarking Scheme Based on Invariant Centroids", Signal Processing and Information Technology, 2007 IEEE International Symposium on
15-18 Dec. 2007 Page(s):190 – 193, 2007.

[36] M. Kutter and Petitcolas, "A Fair Benchmark for Image Watermarking Systems," Electronic Imaging '99: Security and Watermarking of Multimedia Content, SPIE Proc., vol. 3657, San Jose, Jan. 1999.

[37] Husrev Taha Sencar and Nasir Memon, "Combatting Ambiguity Attacks via Selective Detection of Embedded Watermarks", IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, pp. 664-682, December 2007.

[38] Vinay M. Igure, And Ronald D. Williams, "Taxonomies of Attacks And Vulnerabilities in Computer Systems", IEEE Communications Surveys & Tutorials, vol. 10, no. 1, pp. 6-19, 1st Quarter 2008.

[39] Matthew Holliman and Nasir Memon, "Counterfeiting Attacks on Oblivious Block-wise Independent Invisible Watermarking Schemes", IEEE Transactions On Image Processing, Vol. 9, No. 3, Pp 432-441, March 2000.

[40] Thanh-Ha Le, Jessy Clédière, Christine Servière, and Jean-Louis Lacoume Noise, "Reduction in Side Channel Attack Using Fourth-Order Cumulant" IEEE Transactions on Information Forensics And Security, Vol. 2, No. 4, Pp 710-720, December 2007.

[41] Chun-Shien Lu,Hong-Yuan Mark Liao, and Martin Kutter, "Denoising and Copy Attacks Resilient Watermarking by Exploiting Prior Knowledge at Detector", IEEE Transactions on Image Processing, Vol. 11, No. 3, pp. 280-292, March 2002.

[42] Daniel S. Fava, Stephen R. Byers, and Shanchieh Jay Yang, "Projecting Cyber attacks Through Variable-Length Markov Models", IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, pp. 359-369, Sept. 2008 .

[43] Xiangyang Wang, Jun Wu, and Panpan Niu, "A New Digital Image Watermarking Algorithm Resilient to Desynchronization Attacks", IEEE Transactions on Information Forensics And Security, Vol. 2, No. 4, pp. 655-663, December 2007.

[44] Yulin Wang and Alan Pearmain, “Blind MPEG-2 Video Watermarking Robust Against Geometric Attacks: A Set of Approaches in DCT Domain” ,IEEE Transactions on Image Processing, Vol. 15, No. 6, Pp 1536-1543, June 2006.

[45] Bin Yan, Zhe-Ming Lu, and Sheng-He Sun, “Security of Autoregressive Speech Watermarking Model Under Guessing Attack”, IEEE Transactions on Information Forensics And Security, Vol. 1, No. 3, pp. 386- 390, September 2006.

[46] Luis Pérez-Freire, Fernando Pérez-González, Teddy Furon, and Pedro Comesana “Security of Lattice-Based Data Hiding against the Known Message Attack”, IEEE Transactions on Information Forensics And Security, Vol. 1, No. 4, pp. 421-439, December 2006.

[47] Maha El Choubassi, and Pierre Moulin, “On Reliability and Security of Randomized Detectors Against Sensitivity Analysis Attacks”, IEEE Transactions on Information Forensics and Security, Vol. 4, No. 3, pp 273-283, September 2009.

[48] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours, “Spoof Attacks on Gait Authentication System”, IEEE Transactions On Information Forensics and Security, Vol. 2, No. 3, pp. 491-502, September 2007.

Author’s Biography

Dr. Swati Sherekar received the degree of M.Sc. in computer science in 1994 from SGB Amravati University, Amravati. Presently working as Reader in the P. G. Department of Computer Science and having 16 years of teaching experience. Her area of research is Multimedia Network security, Image Processing and completed her Ph.D. in Digital Watermarking for multimedia authentication in 2011. Completed one MRP. Number of papers on her credits at National & International level journals and conferences.

Dr. V.M. Thakare is working as Professor & Head in Computer Science from last 9 years, Faculty of Engineering & Technology, Post Graduate Department of Computer Science, SGB Amravati University, Amravati. He has published 86 papers in various National & International Conferences & 20 papers in various International journals. He is working on various bodies of Universities as a chairman & members. He has guided around 300 more students at M.E / MTech, MCA M.S & M.Phil level. He is a research guide for Ph.D. at S.G.B. Amravati University, Amravati. His interest of research is in Computer Architecture, Artificial Intelligence and Robotics, Database and Data warehousing & mining.