Secure Digital Watermarking-Based Authentication Techniques for Real Time Multimedia Communication

K. Hari Babu Yadav\textsuperscript{1}, G.J. Prakash Babu\textsuperscript{2}, M. Ramesh Babu\textsuperscript{3}, D. Ravi Tej\textsuperscript{4}

\textsuperscript{1}Asst.professor & Head, Dept.of ECE, R.K. College of Engineering, Vijayawada, India.
\textsuperscript{2}Asst.professor, Dept.of ECE, R.K. College of Engineering, Vijayawada, India.
\textsuperscript{3}Asst.professor, Dept.of ECE, R.K. College of Engineering, Vijayawada, India.
\textsuperscript{4}Asst.professor, Dept.of ECE, R.K. College of Engineering, Vijayawada, India.

Abstract – Digital watermarking for multimedia authentication needs for authenticating digital media in this information era and the two main categories of authentication techniques employed to meet these needs, namely labeling-based techniques and watermarking-based techniques. Data integrity and source origin authentication are essential topics for real-time multimedia systems. But the traditional methods are not very applicable to overcome the distortion introduced in multimedia data transportation. In this paper some security mechanics are proposed, which rely on authentication rather than on encryption methods.

The highly asymmetric architectures found in ubiquitous computing applications are exploited to provide a protection of the transmitted multimedia data by means of well known digital watermarking techniques are introduced to meet this need, a content-based image authentication scheme that is suitable for an insecure network and robust to transmission errors. In proposed scheme, The Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and security points of view.

Keywords – Image Content-Based Authenticity Verification, routes, nodes.

I. INTRODUCTION

As the interconnected networks for instant transaction prevail and the power of digital multimedia processing tools for perfect duplication and manipulation increases, forgery and impersonation become major concerns of the information era. As a result, the importance of authentication and content verification became more apparent and acute. In response to these challenges, approaches conveying the authentication data in digital media have been proposed in the last decade. Applications for multimedia authentication can be found in many areas.

For example

- \textit{Imaging / sound recording of criminal events}: Authentic imaging or recording of legally essential event or conversation could lead to breakthrough in criminal cases while maliciously tampered imaging / recording, if not detected, could result in wrong ruling.
- \textit{Broadcasting}: During international crises, tampered or forged media could be used for propaganda and manipulating public opinion. Therefore, broadcasting is an area where multimedia authentication is applicable.

Recent advances in networking and digital media technologies have created a large number of networked multimedia applications. Those applications are often deployed in a distributed network environment that makes multimedia contents vulnerable to privacy and malicious attacks. For insecure environments, it is possible for an enemy to tamper with images during transmission. To guarantee trustworthiness, image authentication techniques have emerged to confirm content integrity and prevent forgery.

These techniques are required to be robust against normal image processing and transmission errors, while being able to detect malevolent tampering on the image [1]. Such authentication techniques have wide applicability in law, commerce, journalism and national defence. The work extending the digital signature scheme from data (fragile or hard) authentication to content (semi fragile or soft) authentication Discovery of routes is a major task. For image authentication, it is desired that the verification method be able to resist content preserving modifications while being sensitive to content changing modifications.
Our main contribution in this paper is to show that the security proof for endair A given in [2] is flawed and that this routing algorithm subject to a hidden channel attack in content-based image authentication over wireless channels. Revisiting the ABV model, we present several reasons why we think that concurrent security for MANET route discovery — i.e., the ABV model’s security standard — is insufficient in practice, because it requires the absence of channels that are always present in any real world MANET application.

II. BACKGROUND

Various types of watermarking schemes have been proposed for different applications. For the purpose of copyright protection, embedded watermarks are expected to survive various kinds of manipulation to some extent, provided that the altered media are still valuable in terms of commercial significance or acceptable in terms of visual quality. On the other hand, in medical, forensic, broadcasting, and military applications where content verification and identity authentication are much more of a concern, more emphases are focused on the capability of the watermarking schemes to detect forgeries and impersonation. This is intended to deal with watermarking schemes for authentication purpose.

A general authentication framework based on digital watermarking is illustrated in Figure 1. Usually, but not always, a secret key $K$ available on both the embedding and authentication sides is used to generate a watermark to be embedded into the host media. The marked media is then delivered via the communication channel (e.g., internet, satellite, etc.) or stored in a database. To authenticate the marked media, the same secret key is used to generate the original watermark so as to be used for extracting and comparing against the embedded version. The difference map, the output of the authentication system, tells the authenticity of the media.

Figure 1. A general authentication framework based on digital watermarking.

2.1 A Watermarking Framework for Real-time Multimedia Communication

Some researchers [3] model the digital watermarking as a kind of communication problem. The technique of digital watermarking can be viewed as modulating a weak noise with a strong signal. If the noise is below a predefined threshold (HVS is a threshold for image watermarking and HAS is a reference measurement for audio watermarking), the distortion introduced by digital watermark can not be noticed by the person.

A typical watermarking framework is first proposed by I. Cox [3], as illustrated in Figure 2. A watermark embedded inserts a digital watermark, $w$, to an original digital media, $D_o$. The watermarked media, $D_1$, should be perceptually identical to the original. The watermarked media may suffer various kinds of attacks during the distribution or transmission. A watermark detector extracts the hidden data, $w'$, from the received copy, $D_2$. The digital watermark may be a message, an image or a video clip. The model is originated from the well known communication model.
Digital watermarking provides an alternative approach to ensure the safety of multimedia data during transmission in openly accessible channels. The digital watermarks may be embedded into the multimedia data to assure its integrity and authenticity without degrading the overall quality of the transmitted data.

Figure 3 shows the outline of a security mechanism using digital watermarks. Digital watermarking operates on the multimedia data to hide/extract information. This makes this approach different to most of the current cryptography mechanisms. When inspecting the integrity and authenticity of the transmitted multimedia data, some special characteristics are to be taken into account - both the amount of the multimedia data and the occurrences of packet loss as well as of bit errors are unpredictable. Since the receiver can only receive the unpredictable multimedia data, we need an independent reference in order to verify the integrity and authenticity of the dynamic multimedia data during transmission. In the proposed approach, the sender and receiver share one reference watermark, $w_1$, from an independent trustworthy party before the multimedia data transmission really starts. To provide the non-repudiate and authenticity, a secret digital watermark, $w_2$, is being introduced. $w_2$ has previously been encrypted with a public key algorithm, e.g., RSA.

The sender embeds both a public, $w_1$, and a secret watermark, $w_2$, into the outgoing multimedia data stream. The receiver then extracts the public digital watermark, $w_1'$, from its incoming stream and compare $w_1'$ with $w_1$ to determine the security of the session. The secret watermark, $w_2$, can be used for the purpose of source origin authentication. This scheme provides an integrated solution to secure multimedia communication and multimedia data integrity.

The network transportation path can be viewed as a noisy channel. The reference digital watermark is modulated with multimedia data (carrier) and transmitted onto the noisy channel. The watermark undergoes the same changes suffered by the multimedia data, so that the watermark degradation can be used to estimate the overall alterations of the multimedia data caused by noise or by attacks. At the receiver side the embedded digital watermark is extracted and compared to the original reference watermark in order to measure the integrity and authenticity of the received multimedia data. It is obvious that the proposed framework integrate the timing mechanism to the multimedia data naturally.

2.2 Applying Digital Watermarking Techniques for Secure Image Capture

Front-ends of image collection systems are in general to be implemented by means of low-cost, low-resource devices. Since this kind of devices embedded into the authentication application feature in most cases a weak computation power only, a straight forward security policies such as encryption is not a good choice. We exploited digital image watermarking technique to this asymmetric computing architecture.

At the front-end’s side, the complete image is first divided into a sequence of images clips $\{I_0, I_1, I_2, \ldots, I_M\}$. The digital watermark, $W$, can also be structured into a sequence of sub-watermarks, $\{W_0, W_1, W_2, \ldots, W_M\}$. Each sub-watermark is then to be inserted into the corresponding image clip in order to create a watermarked
clip. Then the watermarked image clips are sequentially transmitted to the server, which is in charge of image reconstruction and of digital watermark authentication. Finally, the watermark detector of the server extracts a sequence of sub-watermarks denoted as \( \{ \text{W}'_0, \text{W}'_1, \ldots, \text{WM}' \} \) from the received set of marked image clips and decides on the authenticity of the transmitted image. In order to ensure the overall safety of the communication, real-time authentication is employed during the transmission. In the beginning of each transmission cycle, Watermark Embedder on front-end inserts a digital watermark, \( \text{W}_i \), into the \( i \)-th clip of the original image, and then the watermarked clip is sent to Server. As soon as Server receives the watermarked image clip, it extracts the embedded watermark, \( \text{W}'_i \), immediately. Server compares the extracted watermark \( \text{W}' \) with the original one, \( \text{W} \). If \( \text{W}' \) does not differ from \( \text{W} \), then the received image clips are composed into the authenticated final image. After accepting all watermarked image clips, WM_Server reconstructs the full image and checks the authenticity of the received image.

The image watermarking procedure used here is operated in Wavelet Domain. Since DWT is very suitable for low-end chips, the image clip is transformed into wavelet frequency domain first, and then some coefficients are modified slightly to embed the digital watermark into it.

### III. WAVELET PARAMETERIZATION

The generated image’s signature is constructed in the wavelet domain. Wavelet transform is characterized by excellent energy compaction and de-correlation properties; hence, it is employed to effectively generate a compact representation that exploits the structure of the image [13]. Wavelets are also tolerant with respect to color intensity shifts, and can capture both texture and shape information effectively.

Further, wavelet transforms can generally be computed in linear time, thus allowing for fast algorithms [14]. Most conventional wavelet-based image authentication schemes reported in the literature have three shortcomings [13–15]: (1) their security is questionable without protecting the coefficients used to construct the signature from malicious attacks; (2) low robustness to some content preserving attacks; and (3) high computational complexity. To handle the above shortcomings, the concept of lifting based wavelet filter parameterization has been suggested as an effective method to improve the security and processing speed of the wavelet transform [14]. Given \( N \) parameter values \( -\pi < \phi_k < \pi, -\pi < \theta < \pi \), the recursion

\[
\begin{align*}
C_k^N &= \frac{1}{2} \left( C_{k-1}^N + C_{k+1}^N \right) \\
C_{k+1}^N &= \left( -1 \right)^{k+1} \sin \phi_k C_{k-1}^N
\end{align*}
\]

(1)

can be used to determine the filter coefficients \( c_k^N \) for \( 0 < k < 2N + 2 \) and \( c_k^N = 0 \) for \( k < 0 \) and \( k \geq 2N + 2 \). The parameter values used for construction and the resulting wavelet filter coefficients are kept secret. A problem with constructed parametric wavelet filters is that the high-pass/low-pass sub-band property is partially lost [14]. Some degree of wavelet smoothness is desirable for most applications. In this paper, the algorithm used by Fridrich et al. [16] has been considered to deal with this dilemma by calculating the second-order variation of the wavelet sequence

\[
\psi^2 = \sum c_k^N c_k^N - c_k^{N-1} c_k^{N+1}
\]

(2)

as a simple measure to ensure wavelet smoothing. Consequently, the proposed scheme decomposes the host image using a wavelet filter constructed with the above parameterization. Employing secret filter parameterization in image authentication systems has the following advantages [14, 16]. First, security is improved because hostile attacks have to operate in the transform domain used for signing and authentication procedures. Secondly, filter coefficients can be constructed in an image-adaptive manner to maximize robustness against attacks. Thirdly, there is no need to modify proven authentication schemes. A wavelet transform based on secret-adaptive filters can act as a security framework independent of the signing algorithm.

3.1 Structural signature

The proposed scheme uses the same SDS algorithm as used in with the employment of wavelet filter parameterization to increase security. In the wavelet domain of an image, the so-called joint (inter scale) parent–child pairs exist. Each parent–child pair maps to a set of spatial pixels, which is of a non-fixed size and possesses certain contextual dependencies [13]. This dependency
arises from the perceptually important features, for example, edges and textures as illustrated in Fig. 4.

![Fig. 1 Structural signature.](image)

The basic concept of the SDS algorithm relies on the fact [17] that the parent–child pairs with large magnitudes are not vulnerable to attacks, whereas those with smaller magnitudes tend to be easily attacked. Therefore one can use the larger pairs to indicate robustness (content-changing manipulations) and use smaller pairs to reflect fragility (content-preserving manipulations). The construction of an SDS is summarized as follows. Given a pre-determined threshold \( \delta \), select each parent–child pair \((p, j)\) with

\[
K(p, j) \geq \delta
\]  

(3)

the SDS array is recorded as

\[
SDS = \frac{K(p, j)}{\alpha_i} \forall i
\]  

(4)

where \([i, j]\) is a child’s coordinates of significant pairs in the parameterized wavelet domain, and \(\alpha_i\) is defined as

\[
\alpha_i = \begin{cases} 
1: \text{p} > 3, |j| > |i| \\
2: \text{p} < 3, |j| > |i| \\
3: \text{p} > 3, |j| < |i| \\
4: \text{p} < 3, |j| < |i|
\end{cases}
\]  

(5)

Refer to [5] for more details. A comprehensive survey about requirements and implementation of the SDS technique for image authentication is given in [17].

### 3.2 Image authentication procedure

In the image authentication procedure shown in Fig. 4, given corrupted images by transmission and their associated digital signatures, the proposed scheme authenticates both the

![Fig. 4 diagram of the image authentication procedure](image)

integrity and the source of the received image by applying the following process on the image in the following order: (1) perform content-adaptive error concealment, if some blocks are damaged; (2) extract the SDS of the received image using the same method used in image signing; (3) decrypt the signature by using the sender’s public key; (4) perform a content authenticity verification procedure using both the decrypted signature and the extracted one to calculate the degree of authenticity (DY) and un-authenticity (DN); (5) deem the image authenticated if DY > DN; otherwise (6) the attacked areas are detected using an attack detector.

#### 3.2.1 Error concealment

In common wireless scenarios, the image is transmitted over the wireless channel block by block. Because of severe fading, entire image blocks can be lost. Therefore during the verification of image authenticity, error detection and concealment will be carried out. Error concealment techniques are usually applied by either using the contextual relationship of adjacent blocks or through embedded watermarking of information [11]. In this paper, an error concealment algorithm based on edge-directed filters is applied to achieve better visual quality. A
summary of this algorithm is as follows. First, the damaged image blocks are detected by exploring the contextual information in images (e.g. edge continuity). The statistical characteristics of missing blocks are then estimated based on the types of their surrounding blocks. Finally, a directional interpolation strategy for error concealment is applied. Readers looking for more information about this technique refer to [18].

3.2.2 Content Authenticity verification:
For content verification, the proposed scheme implements the same verification procedure used in [10]. The basic idea of this procedure is to use patterns to distinguish distortions by transmission errors from those of attacks, convert these patterns into rules, calculate the degree of authenticity and un-authenticity, and finally obtain the authentication results. As stated in [13,14], the distortion of an attacked image is often concentrated on some content of interest (local distortion), whereas the distortion from transmission is much more randomly distributed over the whole image (global distortion). Furthermore, the attacked areas are more likely to be connected. Therefore the maximum size of the connected modification areas of acceptable manipulation is small, whereas that of the tampering operation is large. From the above facts, given M, the difference map between the extracted SDS (feature vector) from the received image and the decrypted signature associated with the image, the degree of authenticity and un-authenticity is defined as [12].

\[
D_Y = \min (R_Y, R^*_Y) \\
R_Y = \min (1 - R_Y) \tag{6}
\]

Where RI is the degree of global or local distortions, and RY are the degrees of acceptable manipulation size or tampering operation size. RI is computed by

\[
R_I = 1 / (1 + \exp \left( \frac{X^H}{\alpha_T} \right) - b) \tag{7}
\]

Where X and Y are the number of differences in the histogram of horizontal and vertical projections of M, respectively; N is the total number of differences in M; and a and b are constants that are experimentally equal to 100 and 10, respectively, as used in [12], and are defined as

\[
R^*_Y = \begin{cases} 
1 & \text{if } m \geq S \\
\exp \left( \frac{-((m - \bar{S})^2}{2\sigma^2} \right) & \text{otherwise}
\end{cases} \tag{8}
\]

where m is the size of the maximum connected areas in M; L and S denote the large and small sizes, respectively; and \( \sigma^2 = \frac{(L-B)^2}{8} \). Finally, if \( R_Y > R^*_Y \) then the image is classified as authentic; otherwise, tampering areas are detected.

3.2.3 Attack Location
If the image is verified as unauthentic, the attacked locations may be detected using information combining the digital signature and image features. The proposition is based on a feature-aided attack location technique used by [12], which replaces the watermark by an SDS. A summary of this technique is as follows: firstly, morphological operations are used to compute connected areas and remove the isolated blocks and little connected areas. Then the difference map (M) is masked by the union of the SDS and image features. The masking operation can refine the detected areas by concentrating these areas around the objects in the attacked image. Those areas in M which do not belong to an object are removed, which may be a false alarm of some noise or acceptable image manipulations. Such false alarms can be further reduced by removing isolated detected blocks.

IV. WATERMARKING APPROACHES TO AUTHENTICATION

This section is intended to introduce some solutions to the problems posed previously. Several watermarking approaches are discussed as follows.

4.1 Fragile Watermarking Schemes
Among the proposed spatial-domain fragile watermarking techniques, the Yeung - Mintzer scheme [3] is one of the earliest and frequently cited. In [3], the watermark is a visually significant binary logo, which is much smaller than the image to be marked and is used to form a binary image as big as the image. Watermark embedding is conducted by scanning each pixel and performing the watermark extraction function based authentic watermark bit, the pixel is left unchanged; otherwise, the gray scale of the pixel is adjusted until the extracted watermark bit is equal to the authentic one. Because of its pixel-wise scanning fashion, local tampering can be localized to pixel accuracy. The pixel-wise watermarking fashion is actually a special case of the
4.2 Semi-Fragile Watermarking Schemes

One characteristic of the afore mentioned fragile watermarking scheme is their zero tolerance to any types of changes no matter how small they are. This characteristic makes the fragile scheme unsuitable in many applications where content-preserving manipulation is necessary. In order to make efficient use of bandwidth and storage, media are often transmitted or stored in compressed formats according to some specific standards such as JPEG and MPEG. Transcoding is also a common practice to convert media from one format to another (e.g., from JPEG to TIFF). Compression and transcoding are deemed acceptable in many internet and multimedia applications as they preserve the content. However, fragile watermarking schemes do not differentiate content-preserving operations from malicious tampering. Therefore, to meet the needs for authenticating the further compressed or trans-coded watermarked media, it is desirable to have semi-fragile schemes that are sensitive to malicious manipulations while tolerant to content-preserving operations.

V. CONCLUSION

The work described in this paper is concerned with the design of security system for multimedia communication using digital watermarking techniques. An overview of existing watermarking techniques was given and various applications of watermarks were introduced and. Digital watermarking was introduced as an alternative to conventional multimedia security methods.

It represents a first effort toward a formal security model that can deal with concurrent attacks and is successful in mitigating a class of hidden channel attacks. To address this shortcoming, either more flexible definitions of routes must be employed (e.g., redundant routing) or it becomes necessary to address global threats directly, such as those posed by Sybil, wormhole, and more generally, man-in-the-middle attacks. Further work will conduct more tests on the quality of degraded images. Based on the discussions made in the previous sections, it is observed that no single universal solution to all problems is currently in existence and is unlikely to be found in the future. The solutions are more likely to remain application dependent and trade-offs between the conflicting requirements of low distortion, low false positive and negative rates, and robustness to acceptable manipulations still have to be made. The authors expect that the future trends in this field are: increasing the localization accuracy, identify the type of tampering, restoring the original media.

REFERENCES


AUTHORS PROFILE

K. Hari Babu Yadav M.Tech(ECE), working as Asst.Professor & Head in Dept.of ECE at R.K. College of Engineering, Vijayawada, Affiliated to JNTUK, Kakinada, A.P., India. My research interest includes Image processing using MATLAB.

G.J. Prakash Babu M.Tech(ECE), working as Asst.Professor in Dept.of ECE at R.K. College of Engineering, Vijayawada, Affiliated to JNTUK, Kakinada, A.P., India. My research interest includes Image processing using MATLAB.

M. Ramesh Babu pursuing his M.Tech(ECE), working as Asst.Professor in Dept.of ECE at R.K. College of Engineering, Vijayawada, Affiliated to JNTUK, Kakinada, A.P., India. My research interest includes Image processing using MATLAB.

D. Ravi Tej M.Tech(ECE), working as Asst.Professor in Dept.of ECE at R.K. College of Engineering, Vijayawada, Affiliated to JNTUK, Kakinada, A.P., India. My research interest includes Image processing using MATLAB.