A Dynamic Multiple Digital Watermarking Model based on Temporal Logic

Abstract

Information hiding is a typical method to hide messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. When two or more parties communicate, they probably send a series of images rather than a single snapshot, where the main communication content may lie in the images themselves or in the copyright of the images. Therefore, image hiding may involve some rich temporal issues which have been neglected in many approaches to information security. This paper introduces a dynamic multiple digital watermarking model based on a formal characterization of time-series in terms of temporal logic. The security analysis shows that the proposed method of mapping multiple watermarks into a single one overcomes the problem of volume limitation and overlapping of multiple watermarks in a multi-digital-watermarking system.

1 Introduction

With more applications of information hiding, especially watermarking, various techniques have been introduced, such as fragile watermarking and robust watermarking. For the reason that different watermarking techniques have been shown at different stages with different purposes, a new technique, called multiple digital watermarking, has been introduced by others [Koutsouris et al., 2005; Lee, 2009; He et al., 2011]

The multiple digital watermarking techniques are designed for fixing the problems surrounding the copyright certification of a digital product produced by multiple authors when it is released, sold and used. Compared to single watermarking techniques, embedding multiple watermarks is more complicated. It requires that the watermark signals should not interfere with each other through the embedding and detecting procedure. Therefore, the balance between watermark transparency and robustness is a tough issue.

Multiple digital watermarking can be classified into two categories, i.e., static multiple digital watermarking and dynamic multiple digital watermarking. A large amount of work has been done in the field of watermarking [Bansal et al., 1998; Tang et al., 2006]; however, little specific work has been done in the area of dynamic multiple digital watermarking, an exception is that of Tang et al. [Tang et al., 2006]. Other approaches addressing dynamic multiple watermarking actually reflect on the embedding/extracting process [Koutsouris et al. 2005, Lee, 2009; He et al., 2011; Gu and Li, 2008; Zhang et al., 2012], rather than considering temporal issues of the collaborative digital products in an open network. What we shall deal with in this paper in particular is the problem in designing watermarks created by different authors at different times. In a procedure of designing a digital product, especially a procedure that involves collaboration on a product through network protocol, there are often multiple authors. However, not every author designs the product at the same time, which makes it difficult for one to answer, at the start of a product design procedure, the questions of:

(1) Who will collaborate on the product design?

(2) What is the number of authors?

In the highly developed networks of today, it is very common that multiple authors cooperate on a digital product even they don’t know each other. Furthermore, with improvements being made to the product, the number of the authors may also be increasing because such authors are not a team; they work independently and as individuals. As a result, in order to protect the copyrights of the authors, the identity of each author shall be designed into one watermark and be embedded into the digital products.

It is easy to note that at any certain time, even times when the digital product has been released on networks, all the validated watermarks are already embedded into the product. However, it is not possible to predict in advance whether other watermarks, or which watermark, will be embedded. This is a common problem of dynamic multiple digital watermarking: we cannot predict how many watermarks will be embedded in a digital product.

Generally speaking, the notion of time plays a fundamental and important role in the domain of Artificial Intelligence. In particular, it has been noted that time-series are important patterns in sequential modeling of the dynamic aspects of the real world [Das et al, 1997; Guralnik and Srivastava, 1999; Geurts, 2001, Ma, 2008].

The objective of this paper is to introduce a dynamic multiple digital watermarking model. It is based a formal characterization of time-series in terms of temporal logic that is briefly presented in section 2. The scheme of the proposed model is described in section 3. Section 4 presents the results of the corresponding security analysis, which shows the benefit of the proposed method. Finally, section 5 provides the conclusions.

2 The Temporal Basis

As argued in [Ma, 2008], in most approaches to time-series, the fundamental temporal logic based on which time-series are formed up are usually not explicitly specified.

In fact, there has been a longstanding debate in the literature on the issue of what sorts of objects should be taken as the time primitive [Vila, 1994; Ma and Hayes, 2006]. By commonsense, on one hand, points are needed for both theoretical and practical modelling of temporal phenomena. For instance, it is intuitive and convenient to associate punctual events, such as "The image was released at 11:00am" etc., with instantaneous points rather than durative intervals. On the other hand, intervals also seem to be needed for representing temporal phenomena that take up time with positive duration, e.g., "The video played for 30 minutes".

Generally speaking, there are three known objects that may be taken as the time primitive:

- points, i.e., instants of time with no duration;
- intervals, i.e., periods of time with positive duration;
- both points and intervals

However, no matter what a time theory or model is chosen, a temporal order representing the "Before" or "Immediately Before" relationship is needed for defining time-series.

On one hand, in a system based solely on points as primitive like that of Bruce [Bruce, 1972], such a "Before" relation is similar to the classical "Less Than" relation in real number theory; on the other hand, in a system based solely on intervals as primitive like that of Allen's interval temporal logic [Allen, 1981; 1983; 1984], or a system based on both points and intervals like that of Ma and Knight [Ma and Knight, 1994], both of the "Before" and "Immediately Before" relations can be directly expressed by the "Meets" relation [Allen and Hayes, 1989].

N.B. The intuitive meaning of Meets(t_1, t_2) is that, on the one hand, t_1 and t_2 don't overlap each other (i.e., they don't have any part in common, not even a point); on the other hand, there is not any other time object standing between them.

Within a temporal framework based on a chosen temporal logic (either point based, interval based, or point-and-interval based), a time-series ts is defined as a vector of time-elements temporally ordered one after another. Formally, a general time-series is defined in terms of the following schema:

TS.1) ts = [t_1, …, t_n]

TS.2) Meets(t_j, t_{j+1}) $\vee$ Before(t_j, t_{j+1}), for all j = 1, …, n-1

TS.3) Dur(t_k) = d_k, for some k where $1 \leq k \leq n$ and d_i is a non-negative real number, representing the duration of time-element t_k.

where Before(t_1, t_2) $\Leftrightarrow \exists t$(Meets($t_1$, t) $\wedge$ Meets(t, t_2))

Generally speaking, a time-series may be incomplete in various ways. For example, if the relation between t_j and t_{j+1} is "Before" rather than "Meets", it means that the knowledge about the time-element(s) between t_j and t_{j+1} is not available. In addition, if Dur(t_k) = d_k is missing for some k, it means that duration knowledge as for time-element t_k is unknown. Correspondingly, a complete time-series is defined in terms of the schema as below:

CTS.1) ts = [t_1, …, t_n]

CTS.2) Meets(t_j, t_{j+1}), for all j = 1, …, n-1

CTS.3) Duration(t_i) = d_i, for all i = 1, …, n, where d_i is a non-negative real number

3 The Proposed Scheme

Within the discourse of temporal logic, in what follows in this paper, we shall use the following notations:

- [T_1, …, T_m] denotes a time-series.
- At time T_i, the collaborative authors are denoted as A^i_1, A^i_2, …, A^i_{Ni} , where N_i is the number of the collaborative authors.
- The corresponding watermarks for authors A^i_1, A^i_2,…, A^i_{Ni} are denoted as W^i_1, W^i_2, …, W^i_{Ni}, respectively.
- The version of the digital product released at time T_i is denoted as DP_i.
- The single joint watermark for co-authors A^i_1, A^i_2, …, A^i_{Ni} is denoted as W^i.

3.1 Questions and Problems

It is obvious that, every time an author takes part in the product design, one more watermark will need to be embedded in the product. However, since every product has its volume limitation, we cannot embed countless number of watermarks all over the time. As a result, the following Question 1 will occur when we design a multiple digital watermarking technique:

Question 1: How can we overcome the contradiction between the limitation of the image volume and the countless number of watermarks trying to be embedded in?

According to Tang's scheme [Tang et al., 2006], we should solve the problem by embedding only one watermark regardless how many watermarks there will be during the product design process.

However, other questions would then present themselves:

Question 2: Who will map the multiple watermarks to a single watermark? And who will embed it into the image?

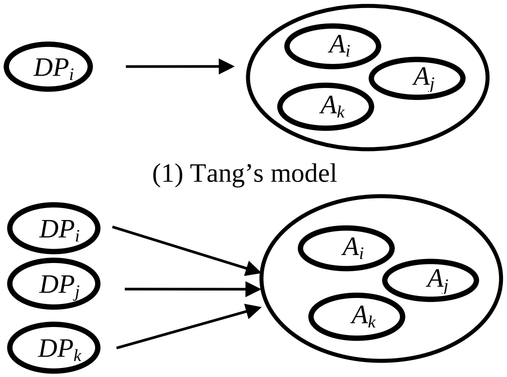
Question 3: How to design such single watermark so that it contains the information of the previous authors as well as the author(s) who will participate in the product?

Question 4: How to design such single watermarks without revealing the plain information of the authors to those who are going to design the watermark?

Question 5: How to make each author to be sure his own watermark has been embedded into the image?

Tang et al. proposed their method in [Tang et al., 2006], but there are some problems that lie in it:

Problem 1: The situation that the current authors may collaborate on the digital product based on multiple previous products has not been considered, i.e., Tang's model can be ascribed by Figure 1 (1), and the proposed model is ascribed by Figure 1 (2).



(1) Tang's model

(2) Our model

Figure 1. Model comparision between Tang's method and the proposed method

Problem 2: The digital product may be produced based on multiple products (different versions of the same product are regarded as different products as well). Therefore, how to generate the watermark for the new product? Who is responsible for embedding the watermark?

In this paper, by means of using an approach that combines with ergodic-matrix based zero-knowledge protocol, we propose a scheme to provide a dynamic multiple digital watermarking technique that improves upon Tang's method and solves the corresponding problems.

At the time T_i when the watermark W^i is about to be inserted in the product DP_{i-1}, the watermark W^{i-1}, which has been embedded in DP_{i-1}, shall be able to authenticate the copyright of all the previous authors. A collaborated digital product work that considers temporal issues (i.e., which work comes first and which comes next) can be drawn into a directed graph as the form shown in Figure 2:

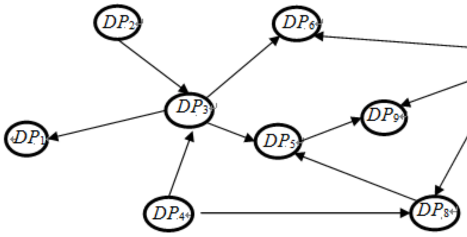


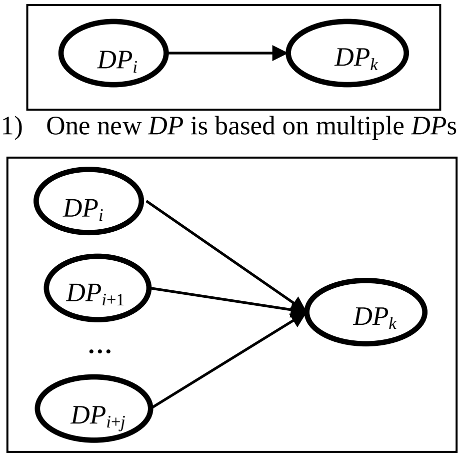
Figure 2. A directed graph describing a collaborated digital product work

The graph is acyclic and unweighted for two reasons:

(1) A new version of the product is generated based on the previous one(s);

(2) Authentication of the product's authors is the main concern, thus the interval time of the two products will not affect the watermarks.

Therefore, the graph should be a DAG (a directed acyclic graph) without weight. Such graph, if only from the view of a new version of *DP*, can be classified into two scenarios, see:



(1) One new *DP* is based on multiple *DP*s

(2) One new *DP* is based on a single *DP*

Figure 3. Two scenarios of a collaborated *DP* work

For Problem 1, there is only one watermark to embed in the product, regardless how many authors are collaborating. Cconsidering the host image's volume and the algorithm complexity, we shall first map the multiple watermarks to a single one and then embed it into the host image. Therefore, from the viewpoint of the authors who are going to design a new product, there is only one scenario, which is (2) in Figure 3. Thus, what we need to be concerned about is how to prevent malicious authors cheating in the watermark. This can be solved by a multi-secret sharing authentication scheme proposed by Wang et. al in [Wang and Qing, 2006]: in the (t, n) secret sharing scheme, a dealer splits a secret into n shares and sends a share to each of n participants. The secret message can be recovered by no less than t members by using a publicly specified algorithm.

After the watermark design, we can apply authentication protocols to identify the ownership of the previous version product and embed the watermark with the safe duplex computing protocol [Tang et al., 2006].

For Problem 2 (see (1) in Figure 3 for reference), the new product is based on the existing products, and each existing product is independent from each other. As a result, it is not appropriate for any of the authors of the existing products to embed the watermark. Therefore, we decide to let the author of the new product to do this work. In this case, there will be various watermarks generated from the new author and any previous authors. Hence, we solve the problem of how to integrate static multiple watermarks into one.

The identification procedure by which Bob identifies whether Alice is the true author is realized by zero-knowledge protocol. The procedure of embedding/extracting watermark can be referred to any watermarking embedding/extracting algorithm.

3.2 Identify the Product's Ownership by Zero-Knowledge Protocol based on Ergodic Matrix

Zero-knowledge protocol is a method for one party to prove to another that a statement (usually a mathematical one) is true, without revealing anything other than the genuineness of the statement [Blum et al., 1988].

Take the example where Alice is the author of DP_1 at time T_1 and Bob is the author at time T_2 ($T_2 > T_1$). Before Bob decides to work on DP_1, he needs to identify whether DP_1 is the genuine product. In other words, he needs to know if Alice is truly the author of DP_1, since Bob doesn't want to be a collaborator in piracy (otherwise he may have to face prosecution for piracy, and also, he may not get paid for the product design).

On the other hand, Alice wishes to protect her copyright through the identification procedure, so that Bob will not be able to cheat when producing the joint watermark (if Bob does, Alice would still have the evidence that Bob admits she is the true author and can then sue him). However in certain cases, such as visual watermark, Alice doesn't want to reveal too much detail of her own watermark W_a. Once the watermark is public, anyone can easily remove the watermark from the host image.

For all the above reasons, we introduce zero-knowledge protocol to prove Alice is the author of DP_1.

Registration Process

① Alice requests identification from Bob, Bob then picks an ergodic matrix Q over finite field $\mathbb{F}^q$ and sends it to Alice;

② Alice encrypts her information by computing $ID_{aa}=Q^{aa}$ and $PWD_a = Q^a$, then he sends (ID_{aa}, PWD_a) to Bob.

③ Bob searches the registration database. If ID_{aa} exists, he will return a message to Alice regarding the failed registration. Otherwise he will create a new record for Alice in the registration database, and will store (ID_{aa}, PWD_a, Q). Thus Alice successfully registers.

Identification Process

① If Alice needs to be identified by Bob, she sends ID_{aa} to Bob.

② Bob checks Alice's ID record in the registration database. If it exists, he will randomly pick an integer s and sends Q^s to Alice.

③ Alice computes $ID_{aa}' = (Q^s)^{aa}$ and sends ID_{aa}' to Bob.

④ Bob then computes $ID_{aa}''=(ID_{aa})^s= (Q^{aa})^s$ and compares ID_{aa}' with ID_{aa}''.

⑤ If they match, Bob will further identify Alice's password PWD_a by the following steps: Bob picks an integer s and sends Q^s to Alice; Alice computes $PWD_a' = (Q^s)^a$ and sends PWD_a' to Bob; Bob then computes $PWD_a''=(PWD_a)^s= (Q^a)^s$ and compares PWD_a' with PWD_a'' and if they match, Alice is successfully identified.

3.3 Joint Watermark Generation

A joint watermark can be generated by a trusted institution, and can also be generated by the communication parties. The former technique is easier to realize: to achieve the joint watermark, Alice and Bob send their watermarks to a trusted institution, then the institution produces a watermark according to the features of Alice and Bob's watermarks, such as by the formula (1):

$$\begin{cases} W_c(i,j) = 1, & if\ W_a(i,j) \geq W_b(i,j) \\ W_c(i,j) = 0, & if\ W_a(i,j) < W_b(i,j) \end{cases} \quad (1)$$

where $W_a(i,j)$, $W_b(i,j)$, $W_c(i,j)$ is the pixel value of Alice's watermark, of Bob's watermark and of the joint watermark, respectively.

If not involved with a third party, plus if Alice and Bob do not want to reveal their own watermark, how do they generate a joint watermark?

Yao's protocol

In [Tang et al., 2006], Tang et al argues that the joint watermark can be produced with Yao's protocol [Yao, 1982]. Yao's protocol is described as follows:

For definiteness, suppose Alice holds an integer i and Bob holds j, where $1 <i, j< 10$. Let M be the set of all n-bit nonnegative integers, and Q_n be the set of all bijections (i.e.,1-to-1 onto functions) from M to M. Let E_a be the public key of Alice, generated by picking a random element from Q_n. The protocol proceeds as follows:

① Bob picks a random n-bit integer Int, and computes $EInt = E_a(Int)$ with Alice's public key;

② Bob sends Alice the number $EInt - j + 1$;

③ Alice computes the following 10 values of $y_u = D_a(EInt-j + u)$ for $u = 1, 2, . . . , 10$.

④ Alice generates a random prime p of $n/2$ bits, then computes the values $z_u = y_u \pmod p$ for all u; if $|z_u- z_v| \geq 2$ for all $u\neq v$, stop; otherwise generates another random prime and repeat the process until all z_u differ by at least 2;

⑤ Alice sends the prime p and the following 10 numbers to Bob: $z_1, z_2, . . . , z_{i,} z_i + 1, z_{i+1} +1, z_{i+2} +1, . . . , z_{10} + 1$;

⑥ Bob checks the j-th number (not counting p) sent from Alice, and decides that $i\geq j$ if $z_j = x \bmod p$, otherwise $i<j$.

⑦ Bob tells Alice the conclusion.

The most useful element of this protocol is that it enables two parties to properly decide who holds the bigger number without knowing each other's detailed information. However the biggest drawback is that Bob may refuse to tell Alice his conclusion or may even lie to her.

In Tang et. al's scheme, they argue their proposed scheme does not need to worry about this issue because Bob's refusing to tell or lying about the conclusion to Alice is simply for the purpose of infringing Alice's ownership. However, Bob has confirmed Alice's copyright before the joint watermark is generated, thus he has no need to do so.

As a result, based on Yao's protocol, Tang's scheme [Tang et al., 2006] and ergodic matrix, we propose a hybrid protocol to produce the joint watermark as follows:

- Generation of the session keys. Alice and Bob agree on a session key.
- Alice and Bob encrypt their watermarks by the session key, hence they get the encrypted watermark W_a' and W_b', respectively.
- W_a' and W_b' are taken respectively as i and j, with Yao's protocol and formula (1), the joint watermark W_{ab} is generated.

3.4 The Temporal Model for Watermark Embedding

No matter how many authors collaborate on a digital product, from the view of the new authors, there are only two scenarios, as shown in Figure 3. Since the watermarks of multiple digital products can be integrated into one with static multiple digital watermarking technique, the scenarios can be simplified into one, i.e., the scenario involves only two watermarks: the watermark of the previous authors and the watermark of the new authors.

Given $(A_1^i, A_2^i, \ldots, A_{N_i}^i)$, $(A_1^{i+1}, A_2^{i+1}, \ldots, A_{N_{i+1}}^{i+1})$, $\cdots$, $(A_1^j, A_2^j, \ldots, A_{N_j}^j)$ are the authors of DP_i, DP_{i+1},$\cdots$, DP_j at time T_i, T_{i+1}, $\cdots$, T_j, respectively. Here $i,j \in \mathbb{N}$ and $i<j$. All of the watermarks have been properly embedded in the products by time T_{i+j}.

Later, at time T_k, authors $(A_1^k, A_2^k, \ldots, A_{N_k}^k)$ wish to design DP_k based on DP_i, DP_{i+1},$\cdots$, DP_j, in this case, the multiple watermarks, W_{ik}, $W_{(i+1)k}$, $\cdots$, W_{jk} (designed by the watermarks between $(A_1^i, A_2^i, \ldots, A_{N_i}^i)$ and $(A_1^k, A_2^k, \ldots, A_{N_k}^k)$, $(A_1^{i+1}, A_2^{i+1}, \ldots, A_{N_{i+1}}^{i+1})$ and $(A_1^k, A_2^k, \ldots, A_{N_k}^k)$, $\cdots$, $(A_1^j, A_2^j, \ldots, A_{N_j}^j)$ and $(A_1^k, A_2^k, \ldots, A_{N_k}^k)$, respectively), shall be integrated into one (denoted as W_{ijk}) before they are embedded in DP_k.

Our model is described as follows:

(1) $(A_1^k, A_2^k, \ldots, A_{N_k}^k)$ verifies if $(A_1^i, A_2^i, \ldots, A_{N_i}^i)$, $(A_1^{i+1}, A_2^{i+1}, \ldots, A_{N_{i+1}}^{i+1})$,$\cdots$, $(A_1^j, A_2^j, \ldots, A_{N_j}^j)$ are the true authors of the digital products, but they don't need to verify every author in $(A_1^i, A_2^i, \ldots, A_{N_i}^i)$, $(A_1^{i+1}, A_2^{i+1}, \ldots, A_{N_{i+1}}^{i+1})$,$\cdots$, $(A_1^j, A_2^j, \ldots, A_{N_j}^j)$, because in section 3.1 we have presumed that the secret message can only be recovered by no less than t members. In addition, when there are many co-authors of a product, it will be a huge work to verify all the authors. The number of verifications is $N_i + N_{i+1} + \cdots + N_k$. We presume the authors $(A_1^k, A_2^k, \ldots, A_{N_k}^k)$ only need to verify one author of the digital product, let's say such author A^i is the "representative" of $(A_1^i, A_2^i, \ldots, A_{N_i}^i)$. With the ergodic matrix-based zero-knowledge protocol introduced in section 3.2, each representative author of $(A_1^i, A_2^i, \ldots, A_{N_i}^i)$, $(A_1^{i+1}, A_2^{i+1}, \ldots, A_{N_{i+1}}^{i+1})$,$\cdots$, $(A_1^j, A_2^j, \ldots, A_{N_j}^j)$ is verified by $(A_1^k, A_2^k, \ldots, A_{N_k}^k)$;

(2) Generate multiple watermarks W_{ik}, $W_{(i+1)k}$, $\cdots$, W_{jk} by Yao's protocol;

(3) Generate the joint watermark W_{ijk} from W_{ik}, $W_{(i+1)k}$, $\cdots$, W_{jk};

(4) A^{N_k} is responsible for embedding the watermark W_{ijk} into DP_k. In Tang's paper [Tang et al., 2006], they explain that since the authors A_{Nk} have admitted the authors $(A_1^i, A_2^i, \ldots, A_{N_i}^i)$, $(A_1^{i+1}, A_2^{i+1}, \ldots, A_{N_{i+1}}^{i+1})$,$\cdots$, $(A_1^j, A_2^j, \ldots, A_{N_j}^j)$ are the authors of DP_i, DP_{i+1},$\cdots$, DP_j, they cannot take possession of or make use of the digital product exclusively for themselves.

(5) Extract W_{ijk} when it is needed.

4 Security Analysis

The security of the proposed dynamic multiple digital watermarking model lies in these following aspects: the zero-knowledge protocol, the encrypted watermarks and the joint watermark.

The security of zero-knowledge protocol based on ergodic matrix is as follows:

Ciphertext attack: The attacker intercepts PWD_a and Q, and he wants to get Alice's private key a with $PWD_a = Q^a$. However, since the order of $Q(Q \in \mathbb{F}_{n\times n}^q)$ is q^n-1, this means the private keys a and s are in the range from 0 to q^n-1. Therefore, if q and n are properly set, a and s can be fairly large so that to get a from Q^a is as hard as breaking the discrete logarithm problem.

Disguise attack: The attacker intercepts Alice's identification ID_a, he then disguises himself as Alice. However, since a is Alice's private key and the key space is quite large, he cannot deduce PWD_a, thus he is unable to be identified by Bob.

Resending attack: The attacker intercepts all the information exchanged in an identification process. He then resends the outdated information in order to disguise himself as Alice or Bob. However, since this kind of attack is based on query/response, the identification information changes each time when Alice and Bob communicate. Therefore, the attack fails when the attacker resends $PWD_a' = (Q^s)^a$. Since Bob's private key s is a random number, it changes in each identification process. Thus the attack will be found when Bob compares PWD_a' with PWD_a''.

Replacement attack: This is the most threatening attack. The attacker intercepts (ID_a, PWD_a) when Alice is registering. He then replaces Alice's information with his (ID_{att}, PWD_{att}), and logs in as Alice. Thus he can tamper with or intercept the content of the communication between Alice and Bob. However, this proposed scheme can resist replacement attack, because in this scheme, Alice encrypts her ID by $ID_{aa}=Q^{aa}$.

The security of the encrypted watermark depends on the session keys used by Alice and Bob. This can refer to any paper on watermarking techniques.

The security of the joint watermark mainly lies in Yao's protocol and analysis can be found in [Yao, 1982]. The biggest issue with this protocol is that Bob might refuse to tell or lie about the conclusion. However, since he has confirmed Alice's copyright before the joint watermark is generated, he has no need to do so.

5 Conclusions

In this paper, we propose a dynamic multiple digital watermarking model based on temporal logic. It is shown through the security analysis the method of mapping multiple watermarks into a single one successfully solves the problem of volume limitation and overlapping of multiple watermarks in a multi-digital-watermarking system. As future work, time-series will be extended to general temporal scenarios that include more complicated temporal relations between time-elements, such as those of Allen’s “During”, “Starts”, “finishes” and “Overlaps” [Allen, 1983], etc.

References

[Allen, 1981] J Allen. An interval-based representation of temporal knowledge. In *Proceedings of the 7th Int. Joint Conf. on AI*, pages 221-226, 1981.

[Allen, 1983] J Allen. Maintaining Knowledge about Temporal Intervals. *communication of ACM.*, 26: 123-154, 1983.

[Allen, 1984] J Allen. Towards a General Theory of Action and Time, *Artificial Intelligence*, 23: 123-154, 1984.

[Allen and Hayes, 1989] J Allen and P Hayes. Moments and Points in an Interval-based Temporal-based Logic, *Computational Intelligence*, 5(4): 225-238, 1989.

[Bansal et al., 1998] Monica Bansal, Weiqi Yan, and Mohan S Kankanhalli. Multiresolution scene-based video watermarking using perceptual models. *IEEE Journal on Selected Areas in Communications*, 16: 540–550, 1998.

[Blum et al., 1988] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 103–112, STOC, 1988.

[Bruce, 1972] B Bruce. A Model for Temporal References and Application in a Question Answering Program. *Artificial Intelligence*, 3: 1-25, 1972.

[Das et al., 1997] G Das, D Gunopulos and H Mannila. Finding similar time series. In *proceedings of Principles of Data Mining and Knowledge Discovery*, *In Proceedings of 1st European Symposium*, pages 88-100, Trondheim, Norway, June 1997.

[Geurts, 2001] P Geurts. Pattern extraction for time series classification. In *proceedings of the 5th European Conference on Principles of Data Mining and Knowledge Discovery*, pages 115-127, Freiburg, Germany, September 2001.

[Gu and Li, 2008] Tao Gu and Xu Li. Dynamic digital watermark technique based on neural network. In *Independent Component Analyses, Wavelets, Unsupervised Nano-Biomimetic Sensors, and Neural Networks VI*, 2008.

[Guralnik and Srivastava, 1999] V Guralnik V and J Srivastava. Event detection from time series data, In *proceedings of the 5th ACM SIGKDD Int'l Conference on Knowledge Discovery and Data Mining*, pages 33-42, San Diego, CA, August 1999.

[He et al., 2011] Xingui He, Ertian Hua, Yun Lin and Xiaozhu Liu. Multiple digital watermarking techniques for cad models. *Applied Mechanics and Materials*, Computer-Aided Design, Manufacturing, Modeling and Simulation:703–708, 2011.

[Koutsouris et al., 2005] D Koutsouris A Giakoumaki, S Pavlopoulos. Multiple digital watermarking applied to medical imaging. In *Proceedings of the Annual International Conference of the IEEE EMBS*, 2005.

[Lee, 2009] Gil-Je Lee. A novel multiple digital watermarking scheme for the copyright protection of image. In *Innovative Computing, Information and Control (ICICIC)*, 2009.

[Ma, 2008] J Ma. A Framework for State-based Time-Series Analysis and Prediction. Int. Journal of Computer and Information Science, 9(1): 21-28, 2008.

[Ma and Knight, 1994] J Ma and B Knight. A General Temporal Theory, *The Computer Journal*, 37(2): 114-123, 1994.

[Ma and Hayes, 2006] J Ma and P Hayes. Primitive Intervals Vs Point-Based Intervals: Rivals Or Allies? *the Computer Journal*, 49(1): 32-41, 2006.

[Tang et al., 2006] Ming Tang, Lina Wang, and Huanguo Zhang. A method of designing dynamic multiple digital watermarking. *Application Research of Computers*, 3:28–30, 2006.

[Vila, 1994] L. Vila. A survey on temporal Reasoning in Artificial Intelligence, *AI Communication*, 7: 4-28, 1994.

[Wang and Qing, 2006] Guilin Wang, Sihan Qing. Analysis and Improvement of a Multisecret Sharing Authenticating Scheme. *Journal of Software*. 2006,17(7): 1627-1623

[Yao, 1982] Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, SFCS ’82, pages 160–164, Washington, DC, USA, 1982. IEEE Computer Society.

[Zhang et al., 2012] Li Zhang, Xilan Yan, Hongsong Li, Minrong Chen. A dynamic multiple watermarking algorithm based on dwt and hvs. *Communications, Network and System Sciences*, pages 490–495, 2012.