Journal of Universal Computer Science, vol. 14, no. 2 (2009), 426-443
submitted: 20/10/08, accepted: 25/1/08, appeared: 28/2/09 © J.UCS

On the Design of Secure Multimedia Authentication

Jinwei Wang, Jianmin Lü
(The 28th Research Institute, CETC
Nanjing, P.R. China
wjwei_2004@163.com)

Shiguo Lian
(France Telecom R&D Beijing
Beijing, P.R. China
shiguo.lian@orange-ft.com)

Guangjie Liu
(Nanjing University of Sci. & Tech.
Nanjing, P.R. China
guangj_liu@yahoo.com.cn)

Abstract: At present, the proposed authentication schemes can be classified into three categories. The first category is the watermarking authentication schemes in which the watermark is independent of the multimedia content. The second category is the signature-based authentication schemes in which the signature is generated by the multimedia content and is not embedded into the multimedia content. The third category is the content-based watermarking authentication schemes in which the watermark is generated by the multimedia content. However, there exists the security question in the above-mentioned three categories of the authentication schemes. In this paper, a novel concept that is called "authentication set" is used to analyze the security of the authentication schemes in detail. Several novel concepts on the authentication set are defined, which are called "Cover Authentication Set", "Attack Authentication Set", "Watermark-based Authentication Set" or "Signature-based Authentication Set", "Verified Authentication Set" and "Malicious-attack Authentication Set". According to the relation among the aforementioned sets, the security of the authentication schemes is exploited. Furthermore, a conclusion is drawn according to the analysis result. At the same time the principle that guides the design of the more secure authentication schemes is presented. Finally, as an example, a novel authentication design method based on multi-feature watermarks is proposed according to the design principle. The experimental results prove the validity of the design method and the significance of the guide principle.

Key Words: content-based, watermarking, authentication, authentication set, design principle
Category: H.3.3, H.4.0, H.5.1

1 Introduction

Due to the rapid development of easy-to-copy software, for example, ACDSee and Photoshop, the multimedia manipulation or tampering becomes easier than before. To check whether the multimedia content is manipulated or tampered, it is possible that the multimedia authentication techniques solve the question.

At present, many authentication schemes are proposed, which can be classified into two categories according to the tolerance degree of manipulating the content of the multimedia data, i.e. fragile authentication schemes [Lin 2004, Wong 1998, Lim 2001, Si 2004, Celik 2001, Yin 2002, Ding 2003, Lu et al 2003] and semi-fragile authentication schemes [Kundur 1999, Lin et al 2000, Lu 2003, Lin et al 2001, Maeno 2002, Tang 2004, Zhou et al 2004, Sun 2002, Huang 2004]. The former can verify the integrity of the multimedia content, and however, its drawback is obvious, that is it cannot tolerate common signal processing such as JPEG compression to any possible modification of the content of the multimedia works. Differently, the semi-fragile authentication schemes are rapidly developed and widely used since almost all the applications of multimedia works allow the minor change as long as their content can be proved authentic. The semi-fragile authentication techniques can not only allow the acceptable manipulations, for example, an unintentional processing of mild JPEG lossy compression, but also verify the malicious unacceptable modifications, for example, substituting, deleting and pasting the multimedia content.

These semi-fragile authentication schemes are mainly based on the watermark independent of multimedia works [Kundur 1999, Lin et al 2000, Eggers 2001, Ye et al 2005, Lu and Liao 2001, Lee 2005, Yang 2004] and the content of the multimedia works [Lu 2003, Lin et al 2001, Maeno 2002, Sun 2002, Huang 2004, Lin and Chang 2000, Hu 2005, Queluz 1999, Lin 2001] . The authentication information of the former is the authentication sequence or logo independent of the multimedia content. In [Kundur 1999], a random sequence is embedded into the DWT transform coefficients by quantizing them to integer multiples of a step size. In [Lin et al 2000], the Gaussian sequence is inserted into the upper triangular positions excluding DC coefficients in DCT domain. In [Eggers 2001], a binary authentication sequence is inserted into the DCT coefficients using the scalar Costa scheme (SCS).In [Ye et al 2005], the image feature is first added to the unwatermarked original image. After a pre-fined message independent of the image content is embedded into the original image, the same feature is subtracted from the watermarked image. In [Lu and Liao 2001], by quantizing the wavelet coefficients of an original image as masking thresholds units, two watermarks, a robust watermark for copyright protection and a fragile one for content authentication, are embedded using cocktail watermarking. In [Lee 2005], random mapping scrambles the order of the sub-images with size of 4×4 in a secret key and then by QIM method the watermark is embedded into the largest single value of 8×8 image block which is composed of neighboring 4 blocked of scrambled 4×4 sub-images. In [Yang 2004], a binary logo is inserted as a watermark into the front N DCT coefficients of randomly selected 8×8 sub-image by using the HVS model. However, the main drawback of these schemes is that their security cannot be guaranteed since the watermark is independent of the multimedia content, for example the unwatermarked coefficients can be modified to achieve the change of the image content and the watermark estimated from a watermarked image can be embedded into the other images. It is noted that the sort of the scheme is generally vulnerable to Vector Quantization (VQ) attack.

The authentication information of the latter is extracted from the multimedia content. These authentication schemes can be divided into signature-based schemes [Lu 2003, Queluz 1999, Lin 2001, Wu 2002, Monga 2005] and content-based watermarking schemes [Lin et al 2001, Maeno 2002, Tang 2004, Zhou et al 2004, Sun 2002, Huang 2004, Lin and Chang 2000, Hu 2005, Yu 2004, Ho 2004, Queluz 2002]. In [Lu 2003], a structural digital signature (SDS) is constructed as image authentication using the image content, which is composed of a set of parent-children wavelet coefficient pairs satisfying certain condition. In [Queluz 1999], two labeling methods are proposed, one of which is based on the invariant of the second-order image moments, the other of which is based on the extraction of image edges. In [Lin 2001], the authentication information is formed based on the relationship of the DCT coefficients in 8×8 block pairs using a pre-determined secret mapping function.In [Wu 2002], the authentication information is generated by combining the advantages of the feature-based authentication and the hash-based one. In [Monga 2005], image authentication is obtained using visually significant feature points which are detected in DWT domain by an iterative feature detector. However, the clear drawback of these signature-based schemes is that the authentication information requires extra channel to be transmitted or stored and this will increase the danger of the schemes' security.

In [Lin et al 2001, Lin and Chang 2000], the authentication information described in [Lin 2001] is inserted into the DCT coefficients by the quantization method. In [Maeno 2002], the authentication information based on [Lin 2001] is inserted into the DWT coefficients using random bias and non-uniform quantization to improve the performance of [Lin and Chang 2000]. In [Tang 2004], the watermark extracted form the relation between the neighboring coefficients in the selected wavelet sub-bands is embedded into the middle frequency sub-bands using the dither quantization. In [Zhou et al 2004], the signature extracted form the non-overlapping 16×16 sub-image is encoded by ECC and then is encrypted to form the authentication information. The authentication information is inserted into the DWT coefficients using the quantization. In [Hu 2005, Yu 2004], the feature watermark, which is generated by the low frequency coefficients, is inserted into the middle frequency coefficients using mean quantization method in DWT domain. In [Ho 2004], the feature codes are extracted from each partition which is formed by the chosen coefficients in the nine neighboring of blocks, based on the relative sign and magnitudes of coefficients. The parity of the binary watermark gotten by XORing two feature codes is embedded into the water-markable quantized DCT coefficients. In [Queluz 2002], the authentication information generated by the random order relationship of image projections is embedded into the M non-overlapping sets of N pixels. The content-based watermarking schemes not only make sure that the authentication information is exclusive but also save the extra channel to be transmitted or stored. However, the significant difference between the signature-based schemes and the content-based watermarking schemes is that the embedding process of the former changes the content of the multimedia and degrades the multimedia quality [Lu 2003].

Generally, the semi-fragile authentication schemes should satisfy the following basic six requirements [Lin and Chang 2000, Hu 2005]:

Imperceptibility, which means that the embedding of watermark into the original multimedia should not heavily degrade the perceptual quality. It is only suitable for the watermark-based authentication schemes.

Obliviousness, which means that the extraction of watermark should not reference to the original multimedia. It fits the watermark-based authentication schemes.

Robustness, which means that the scheme is robust against common acceptable signal processing such as JPEG compression and so on. This requirement is only fit for the semi-fragile authentication scheme.

Fragileness, which means that the scheme is fragile to any change of the multimedia content for the fragile authentication scheme and the scheme is fragile to malicious unacceptable manipulations such as cropping and replacement for the semi-fragile authentication scheme.

Location, which shows that the scheme can locate the manipulated area and verify other areas.

Security, which implies that to the watermark-based authentication schemes, the algorithm of watermark generation or watermark embedding must be secure and to the signature-based authentication schemes, the algorithm of signature generation and the extra channel to be transmitted or stored must be secure. Thus, the watermark information to be embedded and the signature must be exclusive, it can not be forged or manipulated, and the watermark extracted from the received multimedia and the signature generation from the received multimedia must be exclusive.

Although all kinds of the multimedia authentication schemes are proposed, their security is easily neglected. In [Fei 2006], the security of the authentication scheme is analyzed, however, the authors only focus on the semi-fragile watermarking authentication scheme and the security for a coding approach. In this paper, the security of the authentication schemes including the watermark-based and signature-based authentication scheme is analyzed in the scope of the fragileness and the robustness. In order to facilitate analyzing the security of the authentication scheme, the concept of the authentication set is proposed. The semi-fragile authentication schemes are discussed in detail by several significant concepts which are cover authentication set, attack authentication set, verified authentication set and malicious-attack authentication set. Through the analysis, the difference between the security of the hypothesis test and the authentication set is found and the conclusion is drawn. And simultaneously, the principle of the authentication design is presented according to the conclusion. As an example, a special design method is proposed according to the design principle. Finally the experimental results prove the validity and significance of the design principle.

The rest of this paper is arranged as follows. In Section 2, the security of the authentication schemes is analyzed, including the semi-fragile content-based authentication schemes, the fragile content-based authentication schemes and the content-independent watermarking authentication schemes. In Section 3, the principle of the authentication design is presented according to the analysis of Section 2. Next an example of the authentication design is introduced using the design principle in Section 4. In Section 5 the conclusion is drawn.

2 Security Analysis

In order to clearly express our idea and analyze the security of the authentication schemes, a rational hypothesis is established, that is to the first and third classes of the multimedia authentication scheme, the watermarked multimedia with no attacks can be exactly and exclusively verified and to the second class of the multimedia authentication scheme, the original multimedia with no attacks can be exactly and exclusively verified. This is the basic requirement of a multimedia authentication scheme.

In the following content of this paper, the security of the second and the third category of the authentication scheme is analyzed and then the security of the first category of the authentication scheme is analyzed.

2.1 Definition of Authentication Set

For simplicity of security analysis, the concept of the cover authentication set (CAS) is presented. The definition of the cover authentication set is as follows.

Definition 1 **Cover Authentication Set** is the set of all the attacked and un-attacked covers. The cover authentication set contains two sub-sets. One subset is called attack authentication set (AAS) and the other is called watermark-based authentication set (WAS) or signature-based authentication set (SAS). In fact, the WAS and the SAS can be both called Verified Authentication Set (VAS). The definitions of these sub-sets are given as follows.

Definition 2 **Attack Authentication Set** is the set of all the original or watermarking covers which are attacked under the condition of certain feature or some features of given original multimedia from the cover authentication set.

Definition 3 **Watermark-based Authentication Set** is the set of all the covers that are verified on the basis of the watermark from the cover authentication set, excluding the original cover and the un-attacked watermarking cover.

Definition 4 **Signature-based Authentication Set** is the set of all the covers that are verified on the basis of the signature from the cover authentication set, excluding the original cover.

There exists possibly the intersection between VAS and AAS. Let V_A denote AAS and V_V denote VAS. To the semi-fragile authentication scheme, the VAS should be in the AAS, that is $V_V \subset V_A$ and to the fragile authentication scheme, the VAS should be the AAS, that is $V_V = V_A$.

2.2 Security Analysis of Content-Based Semi-Fragile Authentication Scheme

The semi-fragile authentication techniques can not only allow the acceptable attacks, for example, an unintentional processing of mild JPEG lossy compression and mild Gaussian noise, but also verify the malicious unacceptable attacks, for example, substituting, deleting and pasting the multimedia content. Obviously, the AAS can be partitioned into two sub-sets, one of which is the covers that are maliciously attacked and unacceptable, called the malicious-attack authentication set, and the other of which is composed of the covers that are unmaliciously attacked and acceptable, called the unmalicious-attack authentication set. Here, the malicious-attack authentication set is only defined.

Definition 5 **Malicious-Attack Authentication Set** is the set of all the original or watermarked covers which are maliciously attacked under the condition of certain feature or some features of given original cover.

According to the basic requirement of semi-fragile authentication schemes, two hypotheses can be established.

H_0: verify the covers which are not maliciously attacked, that is acceptable covers.

H_1: verify the covers which are maliciously attacked, that is unacceptable covers.

According to two hypotheses, two error probabilities are defined, which are false negative probability and false positive probability. The false negative probability (P_{fn}) is the probability that the covers which are maliciously attacked are verified as the covers which are unmaliciously attacked. That is $P_{fn} = (H_0| H_1)$. The false positive probability (P_{fp}) is the probability that the covers which

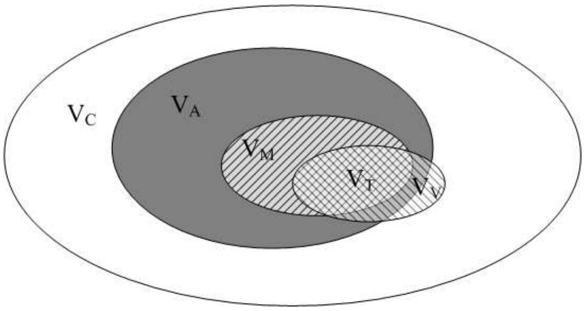

Figure 1: Relation among the authentication sets for the semi-fragile authentication scheme

are unmaliciously are verified as the covers which are maliciously attacked. That is $P_{fp} = (H_1|\ H_0)$.

Here, let λ denote the verified threshold which differentiates from the malicious-attack authentication set and the unmalicious-attack authentication set, which is not less than zero. When λ is equal to zero, the unmalicious-attack authentication set is mull, which is equivalent to $P_{fp} = 1$ and $P_{fn} = 0$; when λ trends to $+\infty$, the malicious-attack authentication set is null, which is equivalent to $P_{fp} = 0$ and $P_{fn} = 1$. It makes sure that the threshold λ is the function on P_{fn} and P_{fp}, that is

$$\lambda = f(P_{fn}, P_{fp})$$

. According to the Neyman-Pearson criterion, the function can be further simplified and rewritten as:

$$\lambda = f(P_{fn}) \text{ or } \lambda = f(P_{fp})$$

.

Now the covers which are maliciously attacked are theoretically verified as all the elements of the VAS according to the basic requirement of the semi-fragile authentication schemes, that is VAS = MAS. However, in fact it have to be noted that the elements of the VAS includes the covers which are given and the other covers which are forged. The covers which are forged in the VAS is called the forged cover. The set of all the forger covers is called the forged authentication set (FAS). The reason of generating FAS is that it can not be guaranteed that the multimedia content is exclusively corresponding to the extracted feature. Therefore, VAS is not actually equal to MAS.

Here, let V_C denote CAS, V_A denote AAS, V_M denote MAS and V_V denote VAS. And then the relationship among these sets is shown in Fig. 1.

The true authentication set V_T is the intersection of V_M and V_V. It should be noted that the result of two above-mentioned hypotheses is different from one of Fig. 1. When considering the verification question from AAS, the result of two hypotheses is obtained and the FAS is ignored. When considering the verification question from CAS, however, the result of Fig. 1 is obtained.

Therefore, two error probabilities P_{fn} and P_{fp} are defined from AAS as follows.

P_{fn} is the probability that v$\in V_M$ and v$\bar{\in} V_V$.

P_{fp} is the probability that v $\bar{\in} V_M$ and v$\in(V_V \cap V_A)$ in AAS.

Here, v represents the element of the set. However, it is found that there exists the area in which v$\bar{\in} V_A$ and v$\in V_V$ in CAS. This area is FAS.

Considering the verification question from CAS, the following two error probability P_{fn} and P_{fp} are defined.

P_{fn} is still the probability that v$\in V_M$ and v$\bar{\in} V_V$.

P_{fp} is the probability that v $\bar{\in} V_M$ and v$\in$V$_V$ in CAS.

The FAS is changed with the change of the chosen multimedia features. When the more and more the multimedia features are chosen, the smaller and smaller the FAS become, that is the possibility that the extracted feature is uniquely corresponding to the multimedia content increases. When the chosen multimedia features are many enough, the FAS may be ignored.

In the next sections, two special classes of the authentication schemes are discussed in detail.

2.3 Security Analysis of Content-Based Fragile Authentication Scheme

In this section, the content-based fragile authentication scheme is classified into two categories, which are the signature-based fragile scheme and the watermark-based fragile scheme. two categories of the schemes are respectively analyzed.

2.3.1 Security Analysis of Signature-Based Fragile Authentication Scheme

In this section, the signature-based fragile authentication scheme is first discussed. It is well known that a digital signature is a set of the multimedia features. Here, assumed that a signature is exclusively generated by a set of the features of the multimedia content and a signature is uniquely projected to the multimedia content uniquely corresponding to the set of the features. Therefore, to the fragile authentication schemes all the multimedia features generate a signature. Ideally, there exists AAS = VAS in the fragile authentication schemes.

Because of the role of verifying the integrity of the multimedia content, two hypotheses are established.

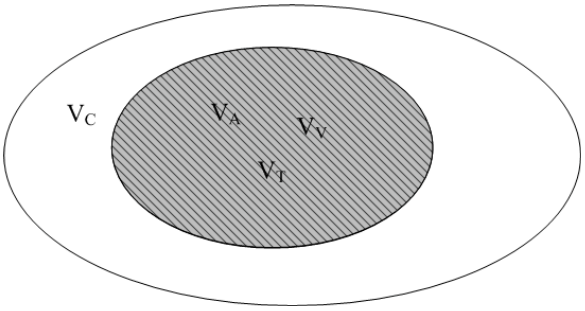

Figure 2: Relation among the authentication sets for the signature-based fragile scheme

H_0: verify the covers that are not attacked, that is the covers are the original covers.

H_1: verify the covers that are attacked.

According to two hypotheses, two error probabilities can be defined. The false negative probability, P_{fn}, is the probability that the covers that are attacked are verified as the covers which are not attacked. The false positive probability, P_{fp}, is the probability that the covers which are not attacked are verified as the covers which are attacked. Because the signature is exclusive to the given multimedia, P_{fn}=P_{fp}=0. This means that the signature-based fragile scheme can be correctly verified and H_1 is accepted as long as the multimedia content can have any change.

If the above-mentioned authentication sets are used to describe the signature-based fragile authentication scheme, the relationship among the authentication sets is shown in Fig. 2.

Observing from Fig. 2, there exists the relationship of V_T=V_A=V_V. Fig. 2 proves that P_{fn}=P_{fp}=0, too.

2.3.2 Security Analysis of the Watermark-Based Fragile Authentication Scheme

In this section, the content-based watermarking fragile authentication schemes are discussed.

Due to the reason why the watermark embedding can not interfere with the extraction of the multimedia features, all the multimedia features can not be used to generate the watermark. But these multimedia features are still more enough to ignore the FAS.

As the above-mentioned description, two hypotheses are established.

H_0: verify the watermarking covers with no attacks.

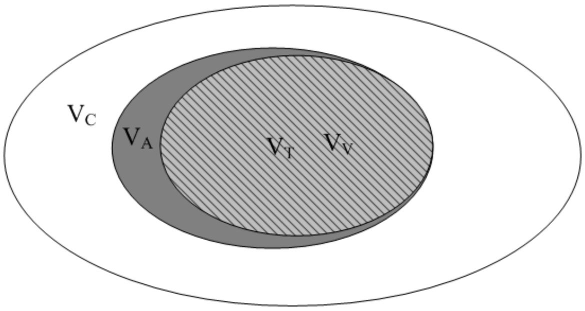

Figure 3: Relation among the authentication sets for the watermark-based fragile authentication scheme

H_1: verify the watermarking covers with the attacks.

Two error probabilities are gotten according to two hypotheses. And finally the result is obtained that the false negative probability, P_{fn}, is equal to 0 but the false positive probability, P_{fp}, is not equal to 0. In order to explain this result, the relationship among the authentication sets is shown in Fig. 3.

There exists the relationship of $V_T = V_V \subset V_A$ in Fig. 3. This means that the false negative probability, P_{fn}, is equal to 0, but the false positive probability, P_{fp}, is achieved the maximum. However, it is noted that to reversible content-based watermarking fragile authentication schemes, the watermark can be generated by all the multimedia features. This tells us the fact that it can obtain the same result as the signature-based fragile authentication schemes, that is $P_{fn} = P_{fp} = 0$.

Actually, we can find that the chosen multimedia features are more enough to achieve the fragileness of the fragile authentication schemes, which is the VAS is equal to the AAS as possible.

2.4 Security Analysis of First Category of Authentication Schemes

It is found through the second and the third category of the authentication scheme which is the content-based authentication scheme, that the first category of the authentication scheme is considered as the special examples of the content-based authentication schemes. The same hypotheses of the first class of the authentication scheme can be established as the second and the third category of the authentication scheme according to the abovementioned analysis, however, the difference between them is obvious, analyzed in detail as follows.

To the fragile authentication schemes, the relationship among the authentication sets is shown in Fig. 4.

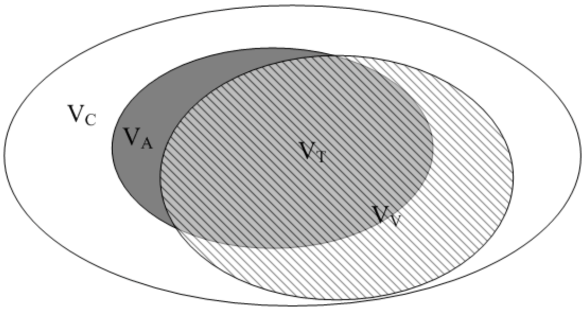

Figure 4: Relation among the authentication sets for the content-independent watermarking fragile authentication scheme

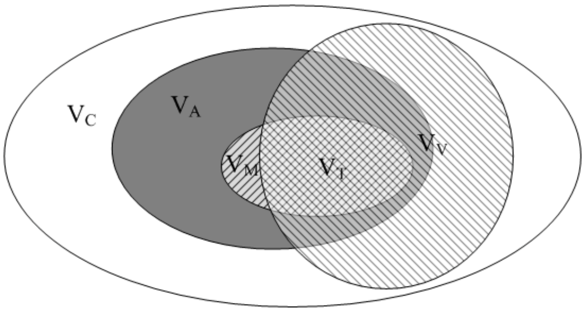

Figure 5: Relation among the authentication sets for the content-independent watermarking semi-fragile authentication scheme

As shown in Fig. 4, the false positive, P_{fp}, is still equal to 0 and the false negative probability is achieved to the maximum, but the FAS become much bigger than one of the content-based fragile authentication schemes, shown in Fig. 5.

To the semi-fragile authentication schemes, the relationship among the authentication sets is shown in Fig. 5.

Pointing to the first class of the authentication scheme, the reason of generating the bigger FAS is that the watermark is independent of the multimedia content and this is just the very important reason why the first class of the authentication schemes are not secure. The content-independent watermark which leads to the authentication leak gives the more chances of forging the watermarking multimedia. A simple example is that the watermarking multimedia can be easily forged by the attacker as long as he can get the watermark information such as logo with the full knowledge of the embedding algorithm.

In fact, the content-based fragile authentication schemes and the first class of the authentication schemes can be thought of two special examples of the content-based semi-fragile authentication schemes if the MAS is taken into consideration. When almost all the multimedia features are used, the semi-fragile authentication schemes become more fragile and make the false positive probability achieve the maximum, and when none of all the multimedia features are used, the semi-fragile authentication schemes become more robust and make the false negative probability and the FAS to achieve the maximum.

Finally we draw the conclusion that the chosen multimedia features in the authentication schemes determine the changes of the false negative probability, the false positive probability and the FAS. In the content-based semi-fragile authentication schemes, if the more multimedia features are chosen, the false negative probability and the FAS will become smaller and simultaneously the false positive probability will become bigger. And if the less multimedia features are chosen in content-based semi-fragile authentication schemes, the false negative probability and the FAS will become bigger and simultaneously the false positive probability will become smaller.

3 Principle of Authentication Design

At present, the single feature is only used in almost of the content-based semi-fragile authentication schemes. However, judged from the above conclusion, it is difficult that the single feature which contains the less multimedia information is satisfactory concerning the requirement of the content-based semi-fragile authentication schemes. To solve the question, multiple multimedia features should be used.

In this paper, the case of two multimedia features is only discussed. And let the verified authentication sets corresponding to two multimedia features respectively denote V_{V1} and V_{V2}, the true authentication sets respectively denote V_{T1} and V_{T2}. So there exist two possibilities in the authentication schemes of two multimedia features, where the intersection of the V_{T1} and the V_{T2} is null set, show in Fig. 6, or not, shown in Fig. 7.

And then to the first possibility shown in Fig. 6, the verified method can only use the union of the V_{V1} and the V_{V2}. However, it is obvious that though the union of the V_{V1} and the V_{V2} make the true authentication set $V_T = V_{T1} \cup V_{T2}$ become big and the false negative probability become small, the false positive negative probability and the FAS become big. Therefore, this verified method can not be adopted.

To the second possibility shown in Fig. 7, there are two verified methods which are the union and intersection of the V_{V1} and the V_{V2}. The disadvantage of using the union of the V_{V1} and the V_{V2} is just said. Now the left method is

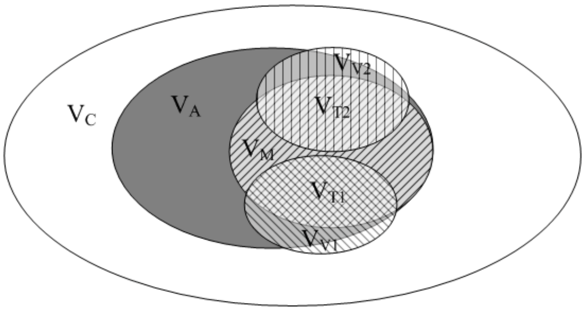

Figure 6: Null set, one of relation among the authentication sets for the multi-feature authentication scheme

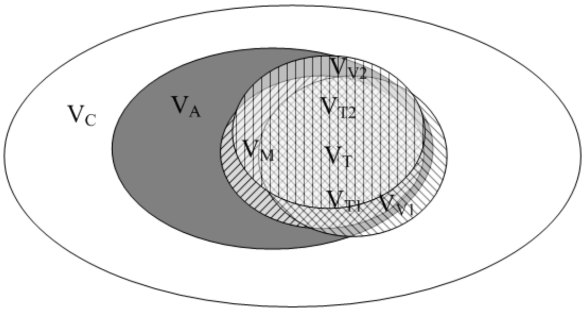

Figure 7: Non-null set, one of Relation among the authentication sets for the multi-feature authentication scheme

the intersection of the V_{V1} and the V_{V2}. But it is found clearly that though the intersection of the V_{V1} and the V_{V2} make the false positive probability and the FAS become small, the true authentication set $V_T = V_{T1} \cap V_{T2}$ become small and the false negative probability become big. Because of the disadvantages of the union and intersection of the V_{V1} and the V_{V2}, the verified method should be designed to achieve the balance between the false positive probability and the false negative probability according to the following requirement.

$$V_{V1} \cap V_{V2} \subset V_V \subset V_{V1} \cup V_{V2}$$

The requirement is the design principle of the verified authentication set. The role of the design principle is to make the true authentication set V_T become big as possible and simultaneously prevent the false positive probability and the FAS from increasing as possible, shown in Fig. 8.

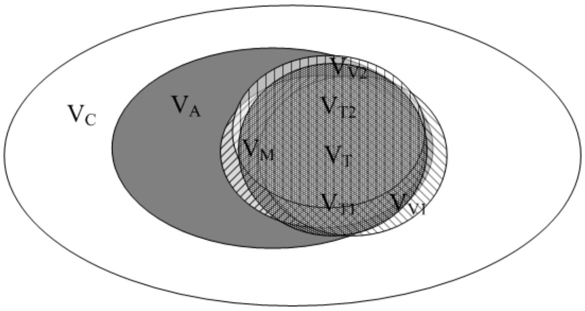

Figure 8: Relation among the authentication sets for multi-feature authentication scheme according to the proposed design principle

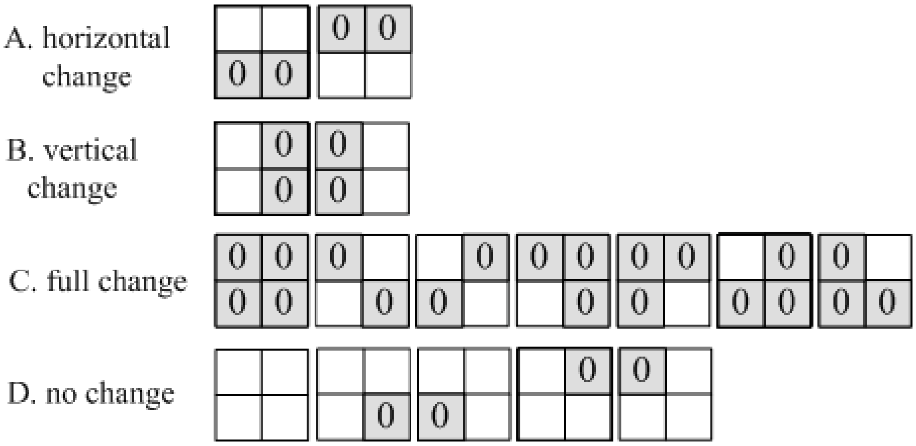

Figure 9: Schematics of marked sub-images

4 Example of Authentication Design

According to the above design principle of the verified authentication set, we use the following method to achieve the requirement.

It is supposed that there are two binary verified feature watermarks W_1 and W_2. The original image is partitioned into the sub-images blocks with size 8×8. When satisfying one of the following four conditions, the sub-image blocks with size 8×8 are marked by 0, representing the modified content. That is, the marked sub-images are classified into four types, which are called horizontal change that is defined as the change of two horizontal sub-images, vertical change that is defined as the change of two vertical sub-images, full change that is defined as

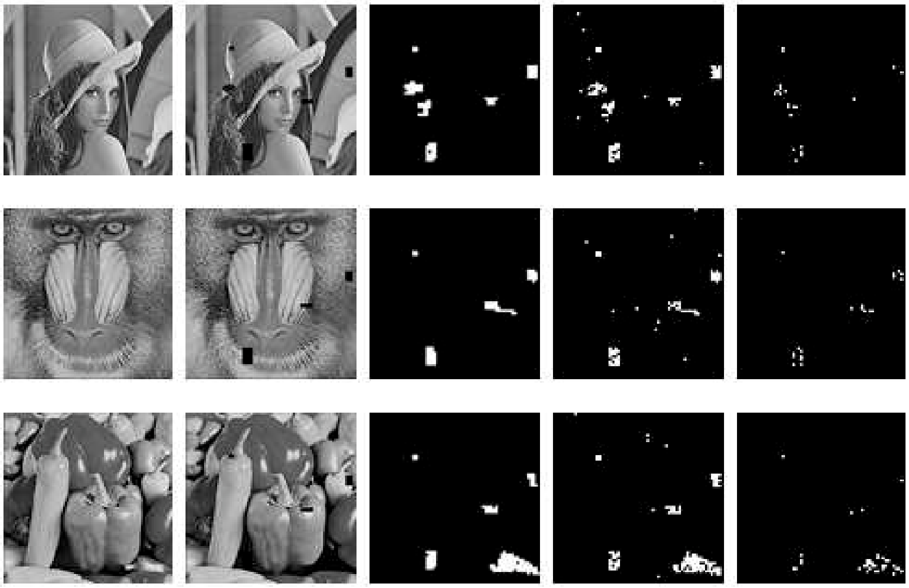

Figure 10: The first column: the original images; the second column: the manipulated watermarking images; the third column: the authentication results using the proposed scheme; the forth column: the authentication results using the union scheme; the fifth column: the authentication results using the intersection scheme

the change of all four sub-images and no change that is defined as no change of all four sub-images. Four types are shown in Fig. 9. The detail description is as follows. The modified sub-images belong to horizontal change when condition (1) is satisfied, the modified sub-images belong to vertical change when condition (2) is satisfied, the modified sub-image belong to full change when one of condition (3) and (4) is satisfied and the modified sub-images belong to no change when no condition satisfies the following four conditions. $W_1(i,j)$ corresponds to the sub-image with size of 8×8 at position (8i, 8j), a gray part represents a sub-image with size of 8×8.

Condition (1): $W_1(i,j) = 1$ and $W_2(i,j+1) = 1$ or $W_1(i,j+1) = 1$ and $W_2(i,j) = 1$;

Condition (2): $W_1(i,j) = 1$ and $W_2(i+1,j) = 1$ or $W_1(i+1,j) = 1$ and $W_2(i,j) = 1$;

Condition (3): $W_1(i,j) = 1$ and $W_2(i+1,j+1) = 1$ or $W_1(i+1,j+1) = 1$ and $W_2(i,j) = 1$;

Condition (4): $W_1(i+1,j) = 1$ and $W_2(i,j+1) = 1$ or $W_1(i,j+1) = 1$ and

$W_2(i+1, j) = 1$.

In order to prove the validity of the design scheme, this proposed scheme [Wang 2008] is compared with the other two schemes which are respectively using the union and intersection of the W_1 and the W_2, called the union scheme and the intersection scheme. In this experiment, the original images with size 512×512 are used, for example, Lena, Barbara, Baboon, Sailboats, Stream and bridge, Peppers, Splash, etc. However, test experiments of three images, Lena, Baboon and Peppers, are listed due to space limitations.

All three test watermarked images we use are cropped at the same four regions selected randomly. Every image is modified according to its characteristic, for example, a flower copied from another image substitutes the original flower in Lena image and the hair of Lena is tampered, a piece of the mustache in the right side of baboon image is deleted and the pepper in the bottom left of peppers image is deleted. The first and second column of Fig. 10 respectively shows five original images and five corresponding modified images.

The comparison results are shown in the third, forth and fifth column of Fig. 10. Observing from Fig. 10, it is found that the proposed scheme obtains the ideal authentication results, the union scheme increases the false positive probability obviously and the intersection scheme increases the false negative probability obviously and decreases the true authentication set V_T obviously.

5 Conclusions

In this paper, lots of the authentication schemes are first partitioned into three categories according to the multimedia contents and the watermarking. The security question of every category is pointed out. Then the novel concept is proposed to analyze the security of the authentication schemes, which is the authentication set. Several concepts on the authentication set, that is the cover authentication set, the attack authentication set, the watermark authentication set, the signature authentication set, the verified authentication set, the malicious-attack authentication set, are defined in detail. Using these concepts, the security of the semi-fragile and fragile authentication schemes are analyzed. Through the analysis result, an important conclusion is drawn that the multimedia features determines the verification result of the authentication process. Furthermore, the principle of the authentication design is presented according to the conclusion. Finally the special scheme is proposed according to the design principle. The validity of the proposed schemes is proved by comparison with the union scheme and the intersection and the experimental results prove the conclusion, too.

In future, the security of the authentication schemes will be further analyzed, and the design principle of the authentication schemes will be improved. A better verified method will be designed according to the proposed principle.

References

[Celik 2001] Celik, M., Sharma, G., Saber, E., Tekalp, A.:"A Hierarchical Image Authentication Watermark with Improved Localization and Security"; IEEE International Conference on Image Processing, Thessaloniki, Greece, 2 (2001) 502-505.

[Ding 2003] Ding, K., He, C., Jiang, L., Wang, H.:"A Novel Fragile Watermark Applying in Verification"; IEEE International Conference on Neural Networks and Signal Processing, Nanjing, Jiangsu China, 2 (2003) 1501-1504.

[Eggers 2001] Eggers, J., Girod, B.:"Blind Watermarking Applied to Image Authentication"; IEEE Interna-tional Conference on Acoustic, Speech, and Signal Processing, Utah USA, 3 (2001) 1977-1980.

[Fei 2006] Fei, C., Kundur, D., Kwong, R.:"Analysis and Design of Secure Watermark-Based Authentication Systems"; IEEE Transactions on Information Forensics and Security, 1, 1 (2006) 43-55.

[Ho 2004] Ho, C., Li, C.-T.:"Semi-Fragile Watermarking Scheme for Authentication of JPEG Images"; Proceedings of the International Conference on Information Technology: Coding and Computing, Las Vegas, 1 (2004) 7-11.

[Hu 2005] Hu, Y.-P., Han, D.-Z.:"Using Two Semi-Fragile Watermark for Image Authentication"; Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou China, 9 (2005) 5484-5489.

[Huang 2004] Huang, P.-M., Wu, D.-C., Tsai, W.-H.:"A Novel Block-Based Authentication Technique for Binary Images by Block Pixel Rearrangements"; IEEE International Conference on Multimedia and Expo, Taipei, Taiwan China, 2 (2004) 903-906.

[Kundur 1999] Kundur, D., Hatzinakos, D.:"Digital watermarking for telltale tamperproofing and authentication"; Proceed-ings of the IEEE Special Issue on Identification and Protection of Multimedia Information, 87, 7 (1999) 1167-1180.

[Lee 2005] Lee, S., Jang, D., Yoo, C.:"An SVD-Based Watermarking Method for Image Content Authentication with Improved Security"; IEEE International Conference on Acoustics, Speech, and Signal Proc-essing, Philadelphia, Pennsylvania USA, 2 (2005) 525-528.

[Lim 2001] Lim, Y., Xu, C., Feng, D.:"Web Based Image Authentication Using Invisible Fragile Watermark"; Proceedings of the Pan-Sydney Area Workshop on Visual Information Processing, Sydney Austra-lia, 11 (2001) 31-34.

[Lin 2001] Lin, C.-Y., Chang, S.-F.:"A Robust Image Authentication Method Distinguishing JPEG Com-pression from Malicious Manipulation"; IEEE Transactions on Circuits and Systems of Video Technology, 11, 2 (2001) 153-168.

[Lin 2004] Lin, P.-L., Huang, P.-W., Peng A.-W.:"A Fragile Watermarking Scheme for Image Authentication with Localization and Recovery"; Proceedings of the IEEE Sixth International Symposium on Multimedia Soft-ware Engineering, Washington, DC, USA (2004) 146-153.

[Lin and Chang 2000] Lin, C.-Y., Chang, S.-F.:"Semi-Fragile Watermarking for Authenticating JPEG Visual Content"; Proceedings of SPIE in Security and Watermarking of Multimedia Contents II, Ping Wah Wong, Edward J. Delp Editors, San Jose, CA USA, 3971 (2000) 140-151.

[Lin et al 2000] Lin, E., Podilchuk, C., Delp, E.:"Detection of Image Alterations Using Semi-fragile Watermarks"; Proceedings of SPIE in Security and Watermarking of Multmedia Contents II, Ping Wah Wong, Edward J. Delp Editors, San Jose, CA USA, 3971 (2000) 152-163.

[Lin et al 2001] Lin, C.-Y., Chang, S.-F.:"SARI: Self-Authentication-and-Recovery Image Watermarking System"; ACM Multimedia, Ottawa, Canada (2001) 628-629.

[Lu 2003] Lu, C.-S., Liao, H.-Y.:"Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme"; IEEE Transactions on Multimedia, 5, 2 (2003) 161-173.

[Lu and Liao 2001] Lu, C.-S., Liao, H.-Y.:"Multipurpose Watermarking for Image Authentication and Protection"; IEEE Transactions on Image Processing, 10, 10 (2001) 1579-1592.

[Lu et al 2003] Lu, H., Shen, R., Chung, F.-L.:"Fragile Watermarking Scheme for Image Authentication"; Electronic Letters, 39, 12 (2003) 898-900.

[Maeno 2002] Maeno, K., Sun, Q., Chang, S.-F., Suto, M.:"New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Non-Uniform Quantization"; Security and Watermarking of Multimedia Contents IV, Edward J. Delp III, Ping W. Wong, San Jose, California USA, 4657 (2002) 659-670.

[Monga 2005] Monga, V., Vats, D., Evans, B.:"Image Authentication Under Geometric Attacks via Structure Matching"; IEEE Conference on Multimedia and Expo, Amsterdam, the Netherlands (2005) 229-232.

[Queluz 1999] Queluz, M.:"Content-Based Integrity Protection of Digital Images"; Part of the IS&T/SPIE Confer-ence on Security and Watermarking of Multimedia Contents, San Jose, California USA, 3657 (1999) 85-93.

[Queluz 2002] Queluz, M.:"Spatial Watermark for Image Content Authentication"; Journal of Electronic Imaging, 11, 2 (2002) 275-285.

[Si 2004] Si, H., Li, C.-T.:"Fragile Watermarking Scheme Based on the Block-Wise Dependence in the Wave-let Domain"; Proceedings of the 2004 Workshop on Multimedia and Security, Magdeburg, Germany (2004) 214-219.

[Sun 2002] Sun, Q., Chang, S.-F., Kurato, M., Suto, M.:"A Quantitative Semi-Fragile JPEG200 Image Authentication System"; IEEE International Conference on Image Processing, Rochester, New York USA, 2 (2002) 921-924.

[Tang 2004] Tang, Y.-L., Chen, C.-T.:"Image Authentication Using Relation Measures of Wavelet Coefficients"; Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Serve (2004).

[Wang 2008] Wang J., Lian, S., Liu, G., Dai, Y., Liu, Z., Ren, Z.:"Secure Multimedia Watermarking Authentication in Wavelet Domain"; Journal of Electronic Imaging, 17, 3 (2008) 033010.

[Wong 1998] Wong, P.-W.:"A Public Key Watermark for Image Verification and Authentication"; Proceedings of IEEE International Conference on Image Processing, Chicago, USA, 1 (1998) 455-459.

[Wu 2002] Wu, C.:"On the Design of Content-Based Multimedia Authentication Systems"; IEEE Transactions on Multimedia, 4, 3 (2002) 385-393.

[Yang 2004] Yang, S., Lu, Z., Zou, F.:"A Novel Semi-Fragile Watermarking Technique for Image Authentication"; 7th International Conference on Signal Processing, Beijing China, 3 (2004) 2282-2285.

[Ye et al 2005] Ye, S., Chang, E.-C., Sun, Q.:"Watermarking Based Image Authentication Using Feature Amplification"; IEEE International Conference on Multimedia and Expo, Amsterdam, the Netherlands, (2005) 610-613.

[Yin 2002] Yin, P., Yu, H.:"A Semi-Fragile Watermarking System for MPEG Video Authentication"; IEEE International Conference on Acoustics, Speech, and Signal Processing, Orlando, Florida USA, 4 (2002) 3461-3464.

[Yu 2004] Yu, S., Hu, Y., Zhou, J.:"Content-Based Watermarking Scheme for Image Authentication"; The 8th International Conference on Control, Automation, Robotics and Vision, Kunming China, 2 (2004) 1083-1087.

[Zhou et al 2004] Zhou, X., Duan, X., Wang, D.:"A Semi-Fragile Watermark Scheme for Image Authentication"; Proceedings of the 10th International Multimedia Modeling Conference, Brisbane Australia (2004) 541-545.