An Improved Version of the Visual Digital Signature Scheme

Abdullah Jaafar and Azman Samsudin
School of Computer Sciences, Universiti Sains Malaysia, Malaysia

Abstract: *The issue of authenticity in data transfer is very important in many communications. In this paper, we propose an improved version of the visual digital signature scheme with enhanced security. The improvement was made based on Yang's non-expansion visual cryptography technique and Boolean operations. The security of the improved version of the visual digital signature scheme is assured by the K-SAT (3-SAT and 4-SAT) NP-hard problem. This is to compare with the security of the existing scheme which is based on the difficulty of solving random Boolean OR operations. Besides improved in security the propose scheme is also, efficient in generating shares, compared to the existing scheme where the probability of generating black shares is high.*

Keywords: *Digital signature, non-expansion visual cryptography, boolean operation, visual share.*

Received November 11, 2011; accepted May 22, 2012; published online August 5, 2012

1. Introduction

A visual digital signature scheme [9] is a new and simple method to enable visual verification of an image without the need to perform heavy and complex cryptographic computations. Instead of generating, computing and manipulating large integers as in the classical digital signature schemes, this method generates shadow images known as visual shares and manipulates them by using the simple Boolean OR operation.

However, the existing visual digital signature scheme has the following drawbacks. First, its security is not based on NP-hard problem. Therefore, we think there is a possibility the method can be attacked. Second, since the existing visual digital signature scheme is using the Boolean OR operation (here OR operation means superimposing the shares), the superimposing of two shares is often resulting in dark image in which there will be more bit 1's than bit 0's. Consequently, the superimposing step in this scheme has to be repeated many times in the process of avoiding from getting full black shares. As the result, the computation cost of this scheme is high.

To overcome the above-mentioned drawbacks, we propose in this paper an improved version of the visual digital signature scheme which the security is based on K-SAT NP-hard problem. The proposed improved scheme in this paper is based on Yang's [15] non-expansion visual cryptography and Boolean operations.

2. Related Work

2.1. Existing Visual Digital Signature Scheme

Jaafar and Samsudin [9], proposed a simple method of visual digital signature, based on the concept of non-expansion visual cryptography. The proposed visual digital signature scheme was built based on simple Boolean OR operation rather than complex calculation as found in conventional digital signature schemes. Thus, the scheme is easily implemented and has a specific niche in visual applications. The visual digital signature scheme is divided into three phases: the initialization phase, signature phase and verification phase. Figure 1 shows the basic idea of the visual digital signature scheme.

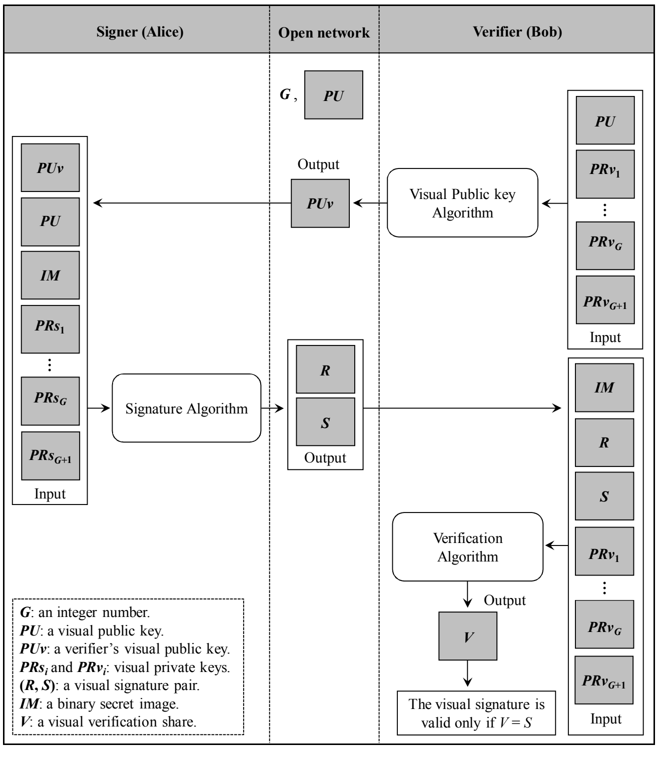

Signer (Alice)
Open network
Verifier (Bob)
G, PU
Output
PUv
Visual Public key Algorithm
PU
PRv1
PRvG
PRvG+1
Input
PUv
PU
IM
PRs1
PRsG
PRsG+1
Input
Signature Algorithm
R
S
Output
IM
R
S
Verification Algorithm
PRv1
PRvG
PRvG+1
Input
Output
V
The visual signature is valid only if V = S
G: an integer number.
PU: a visual public key.
PUv: a verifier's visual public key.
PRsi and PRvi: visual private keys.
(R, S): a visual signature pair.
IM: a binary secret image.
V: a visual verification share.

Figure 1. Visual digital signature scheme (modified from [9]).

2.2. Yang's Non-Expansion (Probabilistic) Visual Cryptography Technique

Yang [15], utilized the conventional Naor and Shamir's visual cryptography method to propose a new visual cryptography technique for binary (black-and-white) images, without pixel expansion. He used the term "probabilistic" to point out that our eyes can recognize the contrast of the recovered image based on the differences of the frequency of white color in black and white areas, where the frequency of white pixels in the white area is higher than that in the black area. In this method, a new parameter $\beta=|p_0-p_1|$ is defined to represent the contrast of the recovered image, where p_0 and p_1 and denote the appearance probabilities of which a white pixel on the recovered image is created from a white and black pixel of the secret image. Each pixel in the original secret image is represented as a black or white pixel in the shares without pixel expansion. The original secret image can be recovered by carefully stacking and aligning the pixels of these shares. Table 1 shows the basic principle of Yang's (2, 2) scheme.

Table 1. Yang's (2, 2) non-expansion visual cryptography scheme.

Pixel of the Secret Image	Share 1	Share 2	Recovered Result	Probability
(White) □	□	□	□	$p_0 = 0.5$
	■	■	■	
(Black) ■	□	■	■	$p_1 = 0$
	■	□	■	

2.3. K-SAT NP-Hard Problem

Hard mathematical problems can be classified into two main categories based on their running time, Polynomial (P) time and Non-deterministic Polynomial (NP) time. The problem is said to be in P if it can be solved by deterministic algorithm in polynomial time, whereas it is in NP if it can be solved by nondeterministic algorithm in polynomial time [10, 11].

The Boolean Satisfiability problem (SAT) is a central problem in combinatorial optimization and it was the first decision problem known as NP-complete, as proved by Stephen Cook in 1971 and independently by Leonid Levin in 1973 [5, 6]. An instance of the problem is a Boolean expression written by using only Boolean variables and logical operations (OR, AND, NOT) on the variables. A special form of SAT is a class of problems which have a fixed number of variables *K*. This class of SAT problem is referred to as K-SAT [13]. An efficient algorithm for solving K-SAT in its worst case instances would immediately lead to other algorithms for efficiently solving thousands of different hard combinatorial problems [2, 7, 12]. 3-SAT and 4-SAT are special cases of K-SAT, which are particularly useful in proving NP-hardness. 3-SAT and 4-SAT will be used in this paper toconstruct the proposed improved scheme.

2.4. Boolean Algebra in K-SAT Format

The K-SAT problem deals with a boolean expression of a set of *n* boolean variables that can take on only two values, True (as digital value 1) and False (as digital value 0), submitted to a set of *m* distinct clauses $C_1,C_2,...,C_m$, where each variable could appear multiple times in the expression. The K-SAT is usually expressed as a boolean expression formula in Conjunctive Normal Form (CNF), where CNF formula is formed by a conjunction of *m* clauses by only the boolean AND operation $(C_1 \wedge C_2 \wedge ... \wedge C_m)$. Each clause C_i consists of only *K* variables, *K* being the uniform clause length, combined by only the Boolean OR operation in the expression. The NP-hard problem is therefore the problem determining whether there exists one configuration of the variables (among the 2^n possible ones) which satisfies all clauses [3, 8, 10].

3. The Proposed Improved Scheme

In this section, a new visual digital signature scheme is proposed based on Yang's non-expansion visual cryptography and Boolean operations (OR and AND). In the proposed method, the verification is done through visual inspection as traditionally being done, rather than through complex mathematical verification procedure. The new improved visual digital signature scheme consists of three phases: initialization, signing generation and verification generation. Before describing the scheme, Table 2 summarizes notations used in this paper.

Table 2. The notations.

Notation	Description
G	An integer number, where $G \geq 2$
PU	A visual public share (common shadow image)
IM_S	A black-and-white secret image intended to be signed
BWI_S	A signer's black-and-white private image uses to generate the visual private keys
PRs_i	The signer's visual private keys, where $i = 1,..., G + 1$
(*R*, *S*)	A visual signature pair generated by the signer
R	The first visual signature share of the visual signature pair (*R*, *S*) generated by the signer
S	The second visual signature share of the visual signature pair (*R*, *S*) generated by the signer
Cs_i	The first intermediate shares in the signing phase for generating the first visual signature share, *R*, of the visual signature pair (*R*, *S*), where $i = 1,..., G$
Ds_i	The second intermediate shares in the signing phase for generating the first visual signature share, *R*, of the visual signature pair (*R*, *S*), where $j = 1,..., G$
Es_i	The first intermediate shares in the signing phase for generating the second visual signature share, *S*, of the visual signature pair (*R*, *S*), where $i = 1,..., G$
Fs_j	The second intermediate shares in the signing phase for generating the second visual signature share, *S*, of the visual signature pair (*R*, *S*), where $j = 1,..., G$
Bs	A full black share (binary matrix) with all elements (pixels) are ones (blacks)
V_1	The first visual verification share generated by the verifier
V_2	The second visual verification share generated by the verifier
HS_B	A verifier's hand signing image
RHS_B	A verifier's recovered hand signing image

3.1. Initialization Phase

This phase is performed by any two communicating parties, the signer (Alice) and the verifier (Bob), who would do the following:

- Alice and Bob agree on a public integer G with $G \geq 2$. There are two reasons in choosing $G \geq 2$. First, the (2, 2) scheme is the basic scheme of the non-expansion visual cryptography which uses two shares to represent the secret information. Secondly, the security of the proposed improved visual digital signature scheme is based on K-SAT NP-hard problem. The K-SAT is a Boolean expression formula which has two components: a set of variables and a set of *m* distinct clauses, where the minimum value of *m* must be at least 2.
- Alice and Bob have agreed on a visual public share (key) PU in the form of $N \times N$ random pixels.
- Alice chooses a black-and-white private image BWI_S with size $N \times N$ pixels and uses Yang's (n, n) non-expansion visual cryptography method as shown in [15] (where n is equal to G+1) to encrypt her private image BWI_S into G+1 visual private shares (keys), PRs_1,..., PRs_{G+1}, where each one is in the form of $N \times N$ pixels, as shown in Figure 2.

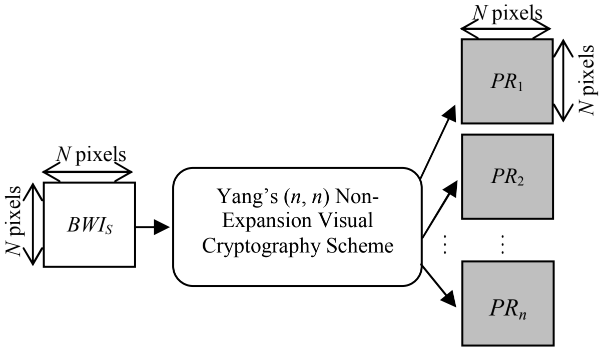


Figure 2. Generation process of the visual private shares (keys).

3.2. Signing Phase

Note that if the signer (Alice) wishes to send the image *IMs* with size $N \times N$ pixels confidentially, first of all, she can use any existing encryption method and then sends it to the verifier (Bob). To sign the image *IMs* in the currently proposed scheme, Alice (the signer) performs the following steps by using only OR (∨) and (^) Boolean operations:

1. She generates the first visual signature share, R, of the visual signature pair (R, S), as follows:

   First, she generates the first intermediate shares (Cs_1,...,Cs_G) of G:

   $$Cs_i = PRs_i \vee PU, \quad i = 1,...,G \tag{1}$$

   Second, she generates the second intermediate shares (Ds_1,…,Ds_G) of G:

   $$Ds_j = PRs_{G+1} \vee Cs_j, \quad i = 1,...,G \tag{2}$$

   Third, she gets the first visual signature share, R, of the visual signature pair (R, S), from the second intermediate shares (Ds_1,…,Ds_G) of G:

   $$R = \bigwedge_{k=1}^{G} Ds_k \tag{3}$$

   Note that the derivation of R is one-way, based on the 3-*SAT NP*-hard problem, where each clause in 3-*SAT* contains exactly three variables.
2. She generates the second visual signature share, S, of the visual signature pair (R, S), as follows:

   First, she generates the first intermediate shares (Es_1,…,Es_G) of G:

   $$Es_i = PRs_i \vee PRs_{G+1} \vee PU, \quad i = 1,...,G \tag{4}$$

   Second, she generates the second intermediate shares (Fs_1,…,Fs_G) of G:

   $$Fs_j = IMs \vee Es_j, \quad i = 1,...,G \tag{5}$$

   Third, she gets the second visual signature share, S, of the visual signature pair (R, S) from the second intermediate shares (Fs_1,…,Fs_G) of G:

   $$S = \bigwedge_{k=1}^{G} Fs_k \tag{6}$$

   Note that, similar to R's case, the derivation of S is one-way and it is based on the 4-*SAT NP*-hard problem, where each clause in 4-*SAT* contains exactly four variables.
3. For preventing the visual verification share V on the Bob's side as we mention later to become full black share Bs if R=Bs or S=Bs, Alice checks visually whether R=Bs or S=Bs; if not, proceeds to step 4; if yes, the signer (Alice) repeats the following two steps until $R \neq Bs$ and $S \neq Bs$.

   - She generates new visual private shares, PRs_1,…, PRs_{G+1}, by choosing a new black-and-white image BWI_S with size $N \times N$ pixels and then repeats the initialization phase as shown in subsection 3.1.
   - She performs steps 1, 2 and 3 as shown in this phase as show in subsection 3.2.
4. She sends the visual signature pair (R, S) of *IMs* to Bob (the verifier).

3.3. Verification Phase

To verify that (R, S) is a valid visual signature of the image *IMs*, the verifier (Bob) carries out the following steps:

1. He generates the first visual verification share, V_1:

   $$V_1 = R \vee IMs \tag{7}$$

2. He checks visually whether V_1=S:

   First, chooses a hand signing image HS_B with size $N \times N$ pixels. Second, generates the second visual verification share V_2 by applying Yang's (2, 2) non-expansion visual cryptography scheme as shown in [15], on HS_B, where share 1 must be equal to the second visual signature share S and share 2 is the second visual verification share V_2 as shown in Figure 3. Third, when V_1=S, then Bob can visually identify the recovered hand signing image RHS_B by superimposing only V_1 and V_2 as follows:

$$RHS_B = V_1 \vee V_2 \tag{8}$$

If the recovered hand signing image RHS_B is approximately equal to the hand signing image HS_B, the verifier (Bob) is convinced that (R, S), which is generated by Alice (the signer), is indeed the valid visual signature of the image IMs. Consequently, equation 8 is true only if V_1=S.

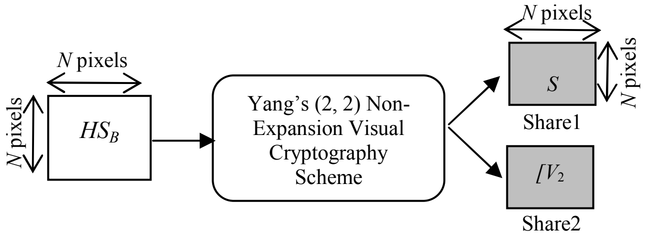


Figure 3. Generation process of the second visual verification share.

Figure 4 shows the basic idea of the proposed improved visual digital signature scheme. The process flow diagram showing the components of the proposed improved visual signature scheme is shown in Figure 5.

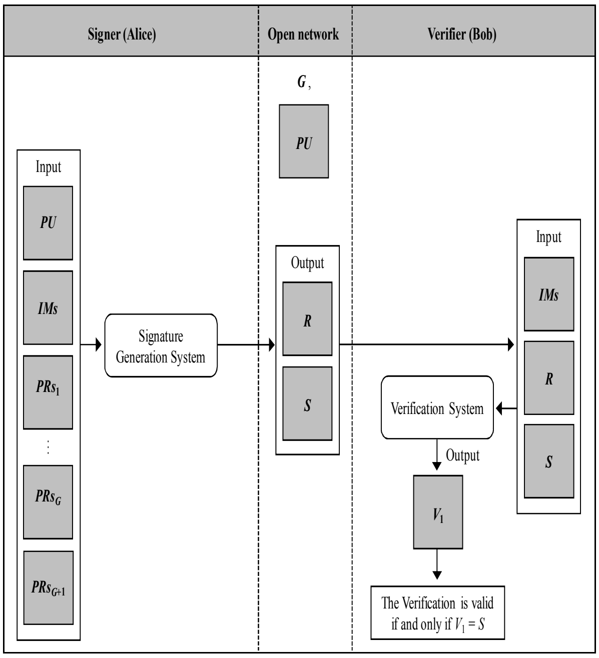


Figure 4. The block diagram of the proposed improved visual digital signature scheme.

- *Theorem 1:* (V_1=S) the verifier's first visual verification share, V_1, is equal to the signer's second visual signature share, S.
- *Proof:* The following shows that the verifier's first visual verification share, V_1, and the signer's second visual signature share, S, are the same (i.e., V_1=S).

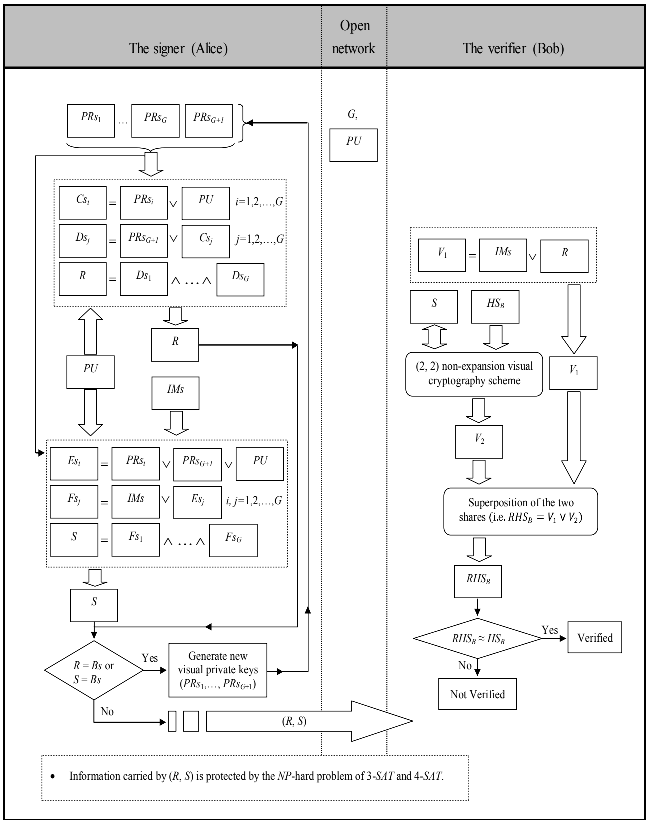

The signer (Alice)
Open network
The verifier (Bob)
PRs_1 … PRs_G PRs_G+1
G,
PU
Cs_i = PRs_i ∨ PU i=1,2,…,G
Ds_j = PRs_G+1 ∨ Cs_j j=1,2,…,G
R = Ds_1 ∧ … ∧ Ds_G
R
PU
IMs
Es_i = PRs_i ∨ PRs_G+1 ∨ PU
Fs_j = IMs ∨ Es_j i, j=1,2,…,G
S = Fs_1 ∧ … ∧ Fs_G
S
R = Bs or S = Bs
Yes
Generate new visual private keys (PRs_1,…, PRs_G+1)
No
(R, S)
V_1 = IMs ∨ R
S
HS_B
(2, 2) non-expansion visual cryptography scheme
V_1
V_2
Superposition of the two shares (i.e. RHS_B = V_1 ∨ V_2)
RHS_B
RHS_B ≈ HS_B
Yes
Verified
No
Not Verified
Information carried by (R, S) is protected by the NP-hard problem of 3-SAT and 4-SAT.

Figure 5. The process flow diagram summarizes the processes of the proposed improved visual digital signature and verification scheme.

3.3.1. The Verifier's First Visual Verification Share (V_1)

$$\begin{aligned} V_1 &= R \vee IMs \\ &= \left(\bigwedge_{i=1}^{G} Ds_i \right) \vee IMs \\ &= \left(\bigwedge_{i=1}^{G} \left(PRs_{G+1} \vee Cs_i \right) \right) \vee IMs. \end{aligned}$$

Because the OR (∨) operation is distributive, we have:

$$\begin{aligned} V_1 &= \left(\bigwedge_{i=1}^{G} Cs_i \right) \vee PRs_{G+1} \vee IMs \\ &= \left(\bigwedge_{i=1}^{G} \left(PRs_i \vee PU \right) \right) \vee PRs_{G+1} \vee IMs. \end{aligned}$$

Because the OR (∨) operation is commutative and distributive, we have:

$$V_1 = \left(\bigwedge_{i=1}^{G} PRs_i \right) \vee PU \vee PRs_{G+1} \vee IMs \tag{9}$$

3.3.2. The Signer's Second Visual Signature Share (S)

$$\begin{aligned} S &= \bigwedge_{i=1}^{G} Fs_i \\ &= \bigwedge_{i=1}^{G} \left(IMs \vee Es_i \right). \end{aligned}$$

Because the OR $(\vee)$ operation is distributive, we have

$$\begin{aligned} S &= IMs \vee \left(\bigwedge_{i=1}^{G} Es_i \right) \\ &= IMs \vee \left(\bigwedge_{i=1}^{G} \left(PRs_i \vee PRs_{G+1} \vee PU \right) \right). \end{aligned}$$

Because the OR $(\vee)$ operation is commutative and distributive, we have:

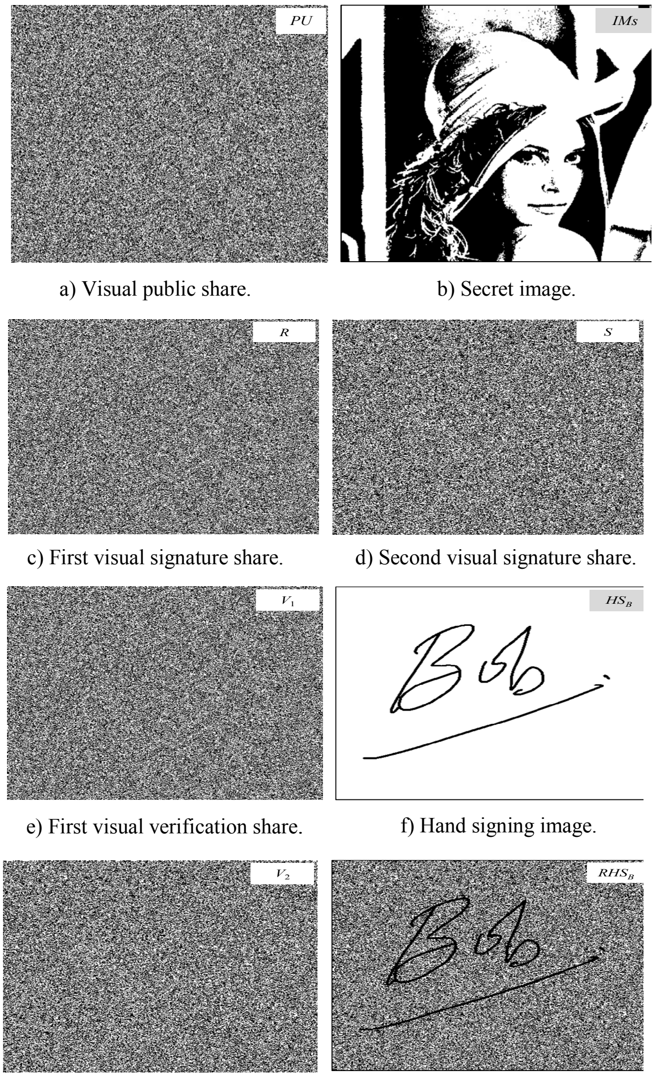
$$S = IMs \vee PRs_{G+1} \vee PU \vee \left(\bigwedge_{i=1}^{G} PRs_i \right) \tag{10}$$

Because the OR operation is associative and commutative, it could be seen from equations 9 and 10 that the verifier's first visual verification share, V_1, and the signer's second visual signature share, S, are the same, namely, V_1=S.

3.4. Working Example

Figure 6 shows a working example of the proposed scheme. In the initialization phase of the scheme, the signer (Alice) and the verifier (Bob) agree on an integer G with $G \geq 2$ and a visual public share PU with size $N \times N$. For simplicity it is assumed that they choose G=4 and a visual public share PU with size 450×450 pixels as shown in Figure 6-a. In addition, on the same phase, the signer constructs G+1 visual private keys (PRs_1, …, PRs_{G+1}) by applying Yang's (n, n) non-expansion visual cryptography scheme, as shown in [15], on her private image BWI_S. In the signing phase of the improved visual digital signature scheme, first of all, supposing that the signer (Alice) chooses the black-and-white original secret image IMs "Lena" with size 450×450 pixels, as shown in Figure 6-b, she applies any existing encryption method on IMs, and then sends IMs to the verifier (Bob). In addition, in the same phase, she generates the visual signature pair (R, S) as shown in Figure 6-c and 6-d and then sends (R, S) to Bob.

In the verification phase, the verifier (Bob) firstly, he generates the first visual verification share V_1 as shown in Figure 6-e and, secondly, he chooses a hand signing image HS_B with size 450×450 pixels as shown in Figure 6-f and generates the second visual verification share V_2 as shown in Figure 6-g by applying Yang's (2, 2) scheme, as shown in [15], on HS_B so, that the first share is equal to the second visual signature share S and the second share is the second visual verification share V_2. If V_1=S, then Bob can visually identify the recovered hand signing image RHS_B, which is approximately equal to the original hand signing image HS_B, by superimposing only V_1 and V_2 as shown in Figure 6-h. Therefore, the verification process of the visual signature is successful. Note that the secret image IMs, the hand signing image HS_B, the recovered hand signing image RHS_B and all the shares in Figure 6 had been resized to fit into a page.



a) Visual public share. b) Secret image.

c) First visual signature share. d) Second visual signature share.

e) First visual verification share. f) Hand signing image.

g) Second visual verification share. h) Recovered hand signing image.

Figure 6. Working example of the proposed improved visual digital signature scheme.

3.5. Security Analysis

Assuming that an adversary may try to obtain the visual private keys (i.e., PRs_1,…, PRs_{G+1}) by using all the information that is publicly available from the proposed improved scheme. In this case, the adversary needs to solve equations 3 and 6 for visual private keys (PRs_1, …, PRs_{G+1}) which are clearly not feasible. This is because:

- First, in equation 3, the first visual signature share of the visual signature pair is defined as $R = \wedge_{i=1}^{G} \left(PRs_{G+1} \vee PRs_i \vee PU \right)$. Since PRs_{G+1} and PRs_i are private values, solving R without the private values is mathematically impossible. Similarly in equation 6, the second visual signature share of the visual signature pair is defined as $S = \wedge_{i=1}^{G} (IMs \vee PRs_i \vee PRs_{G+1} \vee PU)$. Since PRs_i and PRs_{G+1} are private, solving S is mathematically impossible as well if the private values are unknown.

- Second, it is clear that equation 3 is equivalent to 3-SAT NP-hard problem, where *R* is formulated in the Conjunctive Normal Form (CNF).
- Third, equation 6 is equivalent to the 4-*SAT NP*-hard problem, where *S* is also, formulated in *CNF*.

Therefore, the adversary will face difficulties in obtaining the visual private keys from the signer's visual signature pair (*R*, *S*). In addition, if the signer (Alice) has sent the secret image *IMs* to the verifier (Bob) using one of the encryption systems, the adversary will face additional difficulties in obtaining the *IMs* from its encrypted form.

3.6. Computational Complexity

In this subsection, two types of complexities will be discussed: algorithm complexity and brute-force attack complexity on the algorithm. The time complexity in the proposed algorithm is proportional to the share size and to the value of *G*. For the improved scheme, the time complexity for reconstructing a visual signature of an image, *IMs*, is the time required to compute the visual signature pair (*R*, *S*), where the time complexity for computing the first visual signature share, *R*, is $O(N^2G)$ and that for the second visual signature share, *S*, is $O(N^2G)$. Therefore, the sum of the time complexities of the visual signature of an image is $O(N^2G)+O(N^2G)=O(N^2G)$. The time complexity for reconstructing a signature verification of an image is the time required to compute the visual verification shares, V_1 and V_2; where the time complexity for V_1 and V_2 is $O(N^2G)$. Therefore, the sum of the time complexities for the signature verification of an image is $O(N^2G) + O(N^2G)=O(N^2G)$. In addition, the signing phase requires 5*G* stacking (OR operations) of the shares and 2*G*–2 of AND operations. The verification phase also, requires two stacking (OR operations) of the shares.

The proposed improved visual digital signature scheme's time complexities analyzed above are the processes that are being carried out by two parties such as the signer (Alice) and the verifier (Bob). In the case of brute-force attack, the attacker has to find visual private keys from the visual signature pair (*R*, *S*) in order to break the improved visual digital signature scheme. The time complexity of such attack is $O(2^{N^2}G+1)=O(2^{N^2}G)$. If an attacker wishes to compute the signer's visual private keys by using publicly available information (i.e., *G*, *PU*, *R* and *S*); two scenarios (assumptions) are possible:

First, supposing the attack is carried out manually; Table 3 shows the time needed for breaking the visual private keys by brute-force attack when performed by an attacker who is not using any computational devices. Two different sizes of shares are assumed in this case and value of *G* is set to equal to 2, 4, 8 and 16. In this analysis we assume the attacker performs one operation per minute. From the analysis in Table 3 it is clear that such manual brute-force attack is computationally infeasible.

Table 3. The time required for manual brute-force attack.

No.	Share Size (Pixels)	Value G	Number of Operations	Time Required
1	50×50	2	2^{2501}	1.43×10^{747} years
		4	2^{2502}	2.86×10^{747} years
		8	2^{2503}	5.72×10^{747} years
		16	2^{2504}	1.14×10^{748} years
2	55×55	2	2^{3026}	1.57×10^{905} years
		4	2^{3027}	3.14×10^{905} years
		8	2^{3028}	6.28×10^{905} years
		16	2^{3029}	1.25×10^{906} years

As a second scenario, supposing the attack is carried out by a computer; Table 4 shows the time spent for breaking the visual private keys by brute-force attack when performed by an attacker who is using a computational device. Assuming the computer executes two billions instructions per second, similar to the previous scenario, the automate brute-force attack is also, found to be infeasible.

Table 4. The time required for brute-force attack by a computer.

No.	Share Size (Pixels)	Value G	Number of Operations	Time Required
1	50×50	2	2^{2501}	1.19×10^{736} years
		4	2^{2502}	2.38×10^{736} years
		8	2^{2503}	4.76×10^{736} years
		16	2^{2504}	9.53×10^{736} years
2	55×55	2	2^{3026}	1.30×10^{894} years
		4	2^{3027}	2.61×10^{894} years
		8	2^{3028}	5.23×10^{894} years
		16	2^{3029}	1.04×10^{895} years

The time shown in Table 4 indicates only the execution time of operations by a computer. In general, these operations require manual inspection (visually verify the signature) and cannot operate at a high speed, therefore, the results shown in Table 4 are only hypothetical assumptions based on the fact that visual comparison could be made at the rate of two billion operations per second. In both scenarios, the results clearly show that the proposed method is highly secure against the automate brute-force attack. Note that, the time calculations in Tables 3 and 4 are based on complexity analysis and not based on experimentation.

3.7. Comparison with DSA, RSA and the Visual Digital Signature Schemes

Table 5 shows performance comparisons for the proposed improved visual digital signature scheme against DSA, RSA and the original visual digital signature schemes. The four schemes were coded in Turbo C++ 4.5 programming environment and run on a

Table 5. Comparison between DSA, RSA, visual digital signature schemes and the improved visual digital signature scheme.

Scheme			**Hard Problem**	**Brute-Force Complexity**	**Key Length**	**Execution Time (Seconds)**
DSA (code taken from [14])			Discrete logarithm	2^{80} (result taken from [1])	1,024 bits	0.995
RSA (code taken from [4])			Integer factorization			0.752
	Share Size (Pixels)	**Value *G***	No	2^{1028}	1,024 bits	0.332
Visual Digital Signature [9]	32×32	16				
	64×64	8		2^{4099}	4,096 bits	1.006
Improved Visual Digital Signature	32×32	16	K-SAT (3-SAT and 4-SAT)	2^{1028}	1,024 bits	0.278
	64×64	8		2^{4099}	4,096 bits	0.786

personal computer equipped with 2.80 GHz Intel® Pentium 4 CPU, 512 MB of RAM and Windows XP operating system.

The execution time for the improved visual digital signature scheme for 32×32 (or 64×64) pixels binary image and G=16 (or G=8) is generally better than the existing methods as indicated by results shown by Table 5.

4. Conclusions

In this paper, we proposed an improved version of visual digital signature scheme by using Yang's non-expansion visual cryptography technique and Boolean operations. In the new improved scheme, the verification is done through visual inspection as it is traditionally done (hand-signing the document), rather than having to go through complex mathematical verification procedures. The security of the proposed improved scheme is based on the K-SAT (3-SAT and 4-SAT) NP-hard problem. Therefore, the improved scheme is highly secure, particularly when the scheme is used with the proper size of share and the right value of G. When the size of the shares and the value of G are large, the time required to compute the visual private keys from the visual signature pair (R, S) using brute-force attack is computationally prohibitive.

Acknowledgement

The authors would like to thank the School of Computer Sciences at the Universiti Sains Malaysia (USM) for supporting this study.

References

[1] Barker E., Barker W., Burr W., Polk W., and Smid M., *Recommendation for Key Management-Part 1: General (Revised)*, National Institute of Standards and Technology Special Publication, 2007.

[2] Borgulya I., "An Evolutionary Framework for 3-SAT Problems," *Journal of Computing and Information Technology*, vol. 10, no. 3, pp. 185-191, 2003.

[3] Bugacov A., Galstyan A., and Lerman K., "Threshold Behavior in Boolean Network Model for SAT," *in Proceedings of the International Conference on Artificial Intelligence*, Las Vegas, pp. 1-6, 2003.

[4] Cetin K., "Implementation of ElGamal Digital Signatures in C/C++ (ECE 575 Project)," *Data Security and Cryptography*, *Electrical & Computer Engineering*, Oregon State University, 2002.

[5] Cook S., "The Complexity of Theorem-Proving Procedures," *in Proceedings of the 3rd Annual ACM Symposium on Theory of Computing*, New York, pp. 151-158, 1971.

[6] Erickson J., "Lecture 21: NP-Hardness," *Algorithms Course Materials (Revision)*, available at: http://compgeom.cs.uiuc.edu/~jeffe/teaching/algorithms/notes/21-nphard.pdf, last visited 2009.

[7] Garey M. and Ohnson S., *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H. Freeman and Company, New York, 1990.

[8] Giritli M., "From 3-SAT to {2+p}, {3}-SAT," *Master of Logic Thesis*, University of Amsterdam, 2001.

[9] Jaafar A. and Samsudin A., "Visual Digital Signature Scheme: A New Approach," *International Journal of Computer Science*, vol. 37, no. 4, pp. 36-44, 2010.

[10] Menai M. and Batouche M., "Solving the Maximum Satisfiability Problem using an Evolutionary Local Search Algorithm," *International Arab Journal of Information Technology*, vol. 2, no. 2, pp. 154-161, 2005.

[11] Menezes J., Oorschot C., and Vanstone A., *Handbook of Applied Cryptography*, CRC Press, Ontario, 1996.

[12] Mézard M. and Zecchina R., "Random K-Satisfiability Problem: From an Analytic Solution to an Efficient Algorithm," *Physical Review E*, vol. 66, no. 5, pp. 1-38, 2002.

[13] Mitra D., "NP-Complete Problems," available at: http://cs.fit.edu/~dmitra/Algorithms/lectures/NP.doc, last visited 2005.

[14] Walton J., "Cryptographic Interoperability: Digital Signatures," available at: http://www.codeproject.com/KB/security/CryptoInteropSign.aspx, last visited 2009.

[15] Yang N., "New Visual Secret Sharing Schemes using Probabilistic Method," *Pattern Recognition Letter*, vol. 25, no. 4, pp. 481-494, 2004.

Abdullah Jaafar received his PhD degree from School of Computer Sciences, Universiti Sains Malaysia Malaysia, in 2011. He is currently a postdoctoral fellow at the School of Computer Sciences, USM. His research interests include information security (Cryptology), visual cryptography, visual secret sharing Schemes and information hiding-digital steganography.

Azman Samsudin is a lecturer at the School of Computer Sciences, Universiti Sains Malaysia. He received his BSc degree in computer science from University of Rochester, USA, in 1989. He obtained his MSc and PhD degrees in computer science from University of Denver, USA, in 1993 and 1998, respectively. His current research interests are in the fields of cryptography and parallel distributed computing.