A Highly Secure Image Watermarking Authentication Algorithm Based on MECDH and AECDSA

Run Zhang, Yong-Bin Wang, Jin-Yao Yan and Shuang Feng

***Abstract*—This paper proposes a highly secure DSWT (Discrete Stationary Wavelet Transform) domain image watermarking and digital signature algorithm. The algorithm is based on MECDH (Modified Elliptic Curve Diffie-Hellman) key exchange protocol with more secure elliptic curves and SHA-512 AECDSA (Advanced Elliptic Curve Digital Signature Algorithm), both of which are derived from ECC (Elliptic Curves Cryptography) [1] with ECDLP known to be very difficult to solve. Meanwhile, the algorithm run on MIRACL (Multiprecision Integer and Rational Arithmetic C/C++ Library) becomes stronger. Theoretical analyses and experimental results show that the proposed algorithm is more secure and practical to protect the copyrights of multimedia digital works.**

***Index Terms*—AECDSA, ECC, MECDH, MIRACL, Signature Authentication, Watermarking.**

I. Introduction

Watermarking technology with enough imperceptibility, robustness and security is honored as the last defense line of the digital copyright protection. The scheme can resist normal operation as well as malicious attacks, and protect the copyrights and authenticate data integrity. Therefore, digital watermarking technology and products are widely and deeply researched and used. [2] proposed a multiple watermarking technique and made digital assets secure and undetectable by dividing a host image into two regions. It used LSB to insert the owner information in DWT-DFT domain with a circular watermark. [3] proposed a hybrid algorithm combining encryption and digital watermarking techniques which embedded a cryptographic watermark and the users data in the carrier image to provide confidentiality in telemedicine images exchanging.

However, the security of traditional watermarking needs to be improved with currently powerful cryptography technology. Started in 1985, Neal Koblitz and Victor Miller put forward the concept of ECC scheme independently, without noticing the counterpart's existence. Since then, an extensive and deep research on its security and effectiveness has been carried out. Compared to RSA and Diffie-Hellman scheme, ECC with ECDLP has more advantages like higher security, faster calculating speed, less storage space, narrower transmission bandwidth, and deeper mathematical basis and theoretical research. So ECC has become the most powerful public-key mechanism algorithm for its superior security and wider application environment. Meanwhile, ECC also has its disadvantages and may be attacked by the well-known Pollard Rho algorithm [1]. [4] proposed a new method for image tamper detection in the spatial domain. It used authentication encrypted with pseudo random sequence generated by Jacobian elliptic map and then the authentication was embedded in the image.

The problem with [2] is that it didn't use cryptography and authentication technology. Three verification tests were applied in [3].Firstly, ownership authentication with similarity between the extracted watermark and the original watermark. Secondly, integrity verification was employed by comparing the Hash value watermark and the Hash value of the received image's ROI. Finally, tamper location was computed by comparing the CRC-16 value with the extracted CRC-16 value of the same block. But no professional and specific cryptography and digital signature technology are seen. [4] completed a new authentication method based on Jacobian elliptic map with 160 bits key, which was lower robustness and small capacity and easily leaded to reducing the security of watermarking.

To solve the above problem better, our paper proposes more secure algorithms based on MECDH and AECDSA to enforce its security and improve the security of watermarking with the newly proposed algorithms.

The rest of the paper is organized as follows: Section II introduces public-key mechanism with new algorithm based on MECDH and AECDSA. Section III mainly describes the proposed highly secure image watermarking and digital signature with newly proposed scheme. Experimental results and performance analyses are shown in section IV. Finally, we draw some conclusions and discuss the future work.

II. Public-key Cryptography Scheme with New Algorithms Based on MECDH and AECDSA

ECC has been proved to be a more efficient and powerful public-key cryptography scheme, which is based on ECDLP [5]. No algorithm has been found so far with the sub exponential of

Manuscript submitted September 6, 2016. The work was supported by Research, Application and Demonstration of Key Technologies in National Sharing services of Public Digital Culture under Grant 2015BAK25B03.

Run Zhang, Yong-Bin Wang, Jin-Yao Yan and Shuang Feng, are with the Communication University of China, No.1 Dingfuzhuang East Street, Chaoyang District, Beijing, 100024, P.R. China(e-mail: zrun@cuc.edu.cn).

complexity [6]. However, with the deep and new application of ECC, some security problems such as ECDH key exchange protocol and Pollard Rho attack have been revealed gradually. Therefore, we put forward some more secure cryptography and signature algorithm based on MECDH and AECDSA implemented with MIRACL.

A. The Selection of More Secure Elliptic Curves

The security of ECC is on the basis of elliptic curve over finite fields. The elliptic curve with proper parameters is believed to be secure. The more difficult solution to ECDLP is, the more secure the elliptic curve is. The system parameters of secure elliptic curve are open in practice and the security of algorithm has nothing to do with the confidentiality of the parameters. So we'd better follow some essential rules so as to select more secure elliptic curves recommended by the National Institute of Standards and Technology (NIST)[7]. Because the ECC system in our paper studied at software level, the finite field is defined as a prime finite field, $GF(p)$ or F_p.

Let us explain how to choose system parameters for a secure elliptic curve by illustrating the $E(GF(p))$ formed by the points on an elliptic curve defined over a prime finite field.

1) The system parameters of the $E(GF(p))$ expressed as $y^2=x^3+ax+b(mod\ n)$ is commonly described as $D=(p,a,b,G,n,h)$, where $a,b\in GF(p)$, p from $GF(p)$ is a prime number, G is the base point of the curve and the prime n is the order of the point, h is a cofactor meeting the condition of $N=nh$, N is the order of the curve, $\#E(GF(p))$ determined by p, a and b. For being securer, all the parameters in an ECC application are open and required to satisfy the following conditions：The prime $p>3$.
2) $a<p$, $b<p$, $ab\neq 0$, $\triangle=4a^3+27b^2\neq 0$, $(4a^3+27b^2)$ mod $p\neq 0$.
3) $n=\max(2^{191}, 4p^{1/2})$.
4) $h=[\#E(GF(p))]/n$, $1\leq h\leq 4$.
5) $\gcd[p,p+1-\#E(F_p)]=1$ (Non-supersingular).
6) $p+1-2p^{1/2}\leq \#E(F_p)\leq p+1+2p^{1/2}$ [9].
7) $\#E(F_p)\neq p$ (Non-anomalous).

Among all the above parameters, n is the most important, for cryptographically random number and private-key are both taken values from $(1, n-1)$. Thus the length of the ciphers in ECC is normally defined as the binary length of n, which is recommended to be no less than 163 bits [10]. In this paper, for higher security and more receivable response, we choose 192 bits ciphers.

B. MIRACL

MIRACL is a big number library developed by Shamus Software Ltd., and is also the predecessor of the company with the same name as the library. The library not only implements all kinds of the primitives necessary to precisely arithmetical operations of big integer and fraction but also provides relevant algorithms of cryptography based on big number. With all its advantages, MIRACL is widely used in cryptography applications based on ECC. Furthermore, MIRACL runs at fast speed, because of some assembly code in its core.

Therefore, we make full use of the professional big number library to improve the security and the efficiency of highly secure watermarking and authentication resolution proposed in the paper.

C. MECDH (Modified Elliptic Curve Diffie-Hellman)

The ECDH (Elliptic Curve Diffie-Hellman) widely used in Cryptosystems is the key exchange protocol based on ECC and Diffie-Hellman algorithm, but it is vulnerable to Pollard Rho attack. For the purposes of more security, this paper has modified the ECDH and generated the MECDH (Modified ECDH) key exchange algorithm.

The scheme has been implemented in the following manner, which involves the uses of a more secure elliptic curve defined as $E(GF(p))$ with the parameters just like the form of $D=(p,a,b,G,n,h)$ and MIRACL above. The MECDH between two parties, A and B, has been accomplished as follows.

1) Initialization phase
   a) Initializing the MIRACL system for our application with the numbers of digits and the number base, here for 192 and 16 respectively.
   b) Initializing the system parameters, $D=(p,a,b,G,n,h)$, with $GF(\|p\|=192)$ based on secure elliptic curves recommended by NIST.
2) A randomly selects a big integer base on MIRACL, $d_A\in(1, n-1)$, as its private key. Then A computes the corresponding public key, $P_A=d_A\times(G \bmod n)$, which is a point on $E(GF(p))$. Finally A sends its public key, P_A, to B.
3) In the similar way, B randomly selects a big integer, $d_B\in(1,n-1)$, as its private key. Then B computes the corresponding public key, $P_B=d_B\times(G \bmod n)$, which is also a point on $E(GF(p))$. Finally B sends its public key, P_B, to A.
4) A generates the secret key, $K_1=d_A\times P_B \bmod n$. So does B, $K_2=d_B\times P_A \bmod n$, Thus $K=d_A\times d_B\times(G \bmod n)=K_1=K_2$.
5) A randomly selects a big integer as above, $d\in(1, n-1)$, computes $K^*=d\times K$ and sends it to B. So K^* acts as the session secret key.

Compared to the original ECDH key exchange algorithm, the MECDH above makes an attacker fail to get enough information to execute the Pollard Rho attack, and guarantees the new key exchange protocol to perform on unsecure channel.

D. Cryptography with MECDH

With MECDH key exchange protocol mentioned above, we can encrypt plaintext M to ciphertext. For simplicity, let's continue with step C.

1) B randomly selects a big integer as above, $e\in(1, n-1)$, and computes $C_1=e\times K$, $C_2=M+e\times K^*$, here M for plaintext, sends (C_1,C_2) to A.
2) A receives (C_1, C_2) and computes $M=C_2-e\times K^*=C_2-e\times(dK)=C_2-d\times(eK)=C_2-dC_1$.

Based on the MECDH key exchange protocol, the encryption and decryption processing above have improved the security of the original EC EIGamal[11] scheme, with which the Pollard Rho attack could be employed to reveal the private key, leading to potential safety loophole any further.

E. AECDSA (*Advanced Elliptic Curve Digital Signature Algorithm*)

AECDSA with 512 bits signature, implemented on ECC over E(GF(p)) with D=(p,a,b,G,n,h) above and on MIRACL, is the revised edition of the current ECDSA, but more secure with stronger elliptic curves and more efficient with the MIRACL library.

Let's suppose message m to be signed to (m,r,s,t), which is regarded as digital signature to be authenticated.

1) Initialization phase with MECDH above.

2) Signature stage

a) Randomly choose a big integer $d\in(1, \text{n-1})$, which meets the condition of $\gcd(d, n)=1$, as private key, then compute public key, $Q=d\times G$, and makes it public.

b) Compute $e=SHA\text{-}512(m)$ and $w=H(e)$, where SHA-512 is a more secure hash function for 512 bits digest and e is the message digest in the form of MIRACL, w for Hamming weight of e and H for Hamming function.

c) Select a big, random integer, $k\in(1, n\text{-}1)$, which meets the condition of $\gcd(d, n)=1$, then compute $kG=(x_1, y_1)$, $\mathrm{r}=x_1 \bmod n$, $s=(wr+d\text{-}k) \bmod \mathrm{n}$. If $r=0$ or $s=0$ then repeat this step.

d) Select a big, random integer, $\lambda\in(1, n\text{-}1)$, which meets the condition of $\gcd(\lambda, n)=1$, then compute $t=\lambda\times m$, if $t=0$ then repeat the step.

e) Generate the signature (m,r,s,t).

3) Authentication stage

a) Judge the validity of the signature, (m,r,s,t). If $(r, s)\notin (1, n\text{-}1)$ then show that the signature is false.

b) Compute $e=SHA\text{-}512(m)$ and Hamming weight of e, w, then repeat in the same way above.

c) Compute $X=(s\text{-}wr\text{-}\lambda m+u)G +Q=kG=(\mathrm{x}_2,\mathrm{y}_2)$. If $X=O$ then the signature is false else $v=x_2 \bmod n$.

d) If $v=r$ then the signature is validity else invalidity.

The AECDSA algorithm can not only resist kinds of attacks at the ECDSA scheme by forged signature like replacing message or random number, but also reduce the operating quantity.

III. SECURE WATERMARKING ALGORITHM WITH NEW ALGORITHM BASED ON MECDH AND AECDSA

Human Vision System (HVS) is playing an important role in image watermarking scheme. We use the HVS combined with newly proposed algorithms based on ECC and MIRACL to achieve our goal of ideal secure performance of the watermarking algorithm with better balance of invisibility and robustness.

A. Images Preprocessing

1) DSWT

The major weakness of the classical DWT is that it can't provide shift invariance on account of down-sampling of its sub-bands, which means DWT is not a time-invariant and leads to inaccurate extraction of the watermark embedded into a carrier image, possibly results in a poor extracted watermark.

In order to solve the problem, we introduce the DSWT algorithm to this paper. DSWT is designed to aim at overcoming the lack of shift invariance of DWT by removing down-sampling and up-sampling of coefficients during each filter-bank iteration and up-sampling the filter coefficients by a factor of 2^j in the j+1 level of the algorithm [12]. Since frame expansion increases robustness with respect to additive noise, images processing based on DSWT is more robust than that based on DWT [13].

In this paper, a selected carrier image and a selected watermark image with DSWT is implemented by *swt*2 function running on MATLAB R2012b, performing *swt*2 decomposition of the carrier image I at level 2 for higher PSNR and the watermark image W at level 1, generating $LL2$ for approximation coefficients of the carrier image and LL for approximation coefficients of the watermark image respectively.

2) SVD

SVD is used to extract algebraic features from images. Both DSTW and SVD do benefit to HVS in the proposed watermarking algorithm.

Let us suppose that A is a given gray-scale image represented in the form of $m\times n$ matrix with the data type of *single* in MATLAB environment, the result of SVD transformation is described as follows:

$$A=U\times\Sigma\times V^T \qquad (1)$$

Here U is an $m\times m$ *single* unitary matrix, Σ is an $m\times n$ rectangular diagonal matrix with non-negative *single* values on the diagonal, and V^T is an $n\times n$ *single* unitary matrix. The diagonal entries $\Sigma_{i,i}$ of Σ are known as the singular values of A.

SVD transformation efficiently reveals intrinsic algebraic properties of an image, where singular values relate to brightness of an image and singular vectors reflect geometry characteristics of an image [14]. Because singular values concentrate the main energy of an image and singular vectors have good stability and rotation invariance, both of them are useful for invisibility and robustness of the proposed watermarking scheme.

In our paper, the image A in equation (1) is replaced by LL2 and LL subband respectively, both of the subband are transformed according to SVD operation mentioned above.

B. Embed Watermark and Generate Digital Signature

The newly proposed secure watermarking embedding algorithm based on MECDH and AECDSA is implemented with DSWT and SVD in MATLAB environment. The algorithm illustration is shown in Fig. 1.

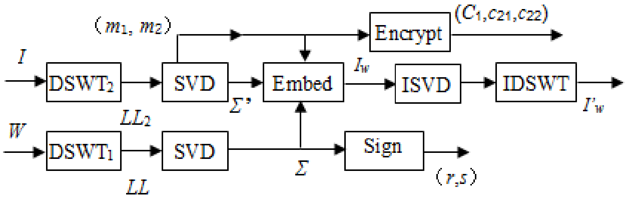


Fig. 1 Watermark Embedding Algorithm

The steps of watermark embedding and digital signature generating algorithm are described as follows:

1) Apply DSWT at level 2 to the carrier image to decompose it into LL_2, HL_2, LH_2, HH_2 sub-bands, and apply SVD transformation to LL_2 to generate its diagonal matrix Σ'.
2) Apply DSWT at level 1 to the watermark image to decompose it into LL, HL, LH, HH sub-bands, and apply SVD transformation to LL to generate its diagonal matrix Σ.
3) Modify the singular values of the carrier image with the singular values of watermark image based on the following expression:

$$I_w=\Sigma'+\sigma\Sigma \qquad (2)$$

Where I_w stands for the watermarked image, σ for embedding intensity coefficient.

4) Encrypt position parameters with MECDH algorithm based on MIRACL.

$(m_1||m_2)$ are encrypted to 192-bit $(C_{1,} C_2)$ in the form of hexadecimal, where m_1 stands for the starting position and m_2 for number of embedding coefficients.

5) Generate 512-bit digital signature (m,r,s,t) based on the AECDSA.
6) Apply inverse SVD and DSWT to the transformed carrier image to reconstruct the watermark-embedded image.

C. Extract Watermark and Authenticate Digital Signature with MECDH and AECDSA

The proposed secure watermark extracting algorithm based on MECDH and AECDSA is implemented with DSWT and SVD in MATLAB environment. The algorithm illustration is shown in Fig. 2. The meanings of the parameters are listed above. As an exception, W'' stands for the extracted watermark image and W' for reconstructed watermark image based on W''.

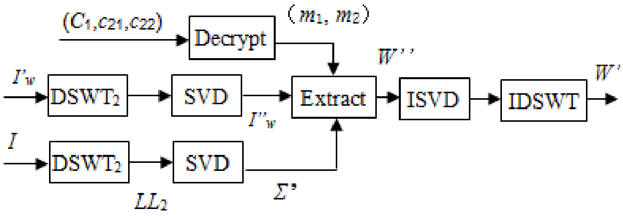


Fig. 2 Watermark Extracting Algorithm

The steps of watermark extracting and authenticating digital signature algorithm based on AECDSA are an inverse process B simply described as follows:

1) Apply $DSWT_2$ and SVD transformation to I'_w to generate $I''_{w.}$
2) Apply $DSWT_2$ and SVD transformation to I to generate Σ'.
3) Decrypt encrypted position parameters (C_1, C_2) to (m_1, m_2) based on the corresponding algorithm above.
4) Extract the singular values from the watermarked image according to the following formula:

$$W''=(I''_w-\Sigma') \qquad (3)$$

5) Apply inverse SVD and DSWT to W'' to obtain the extracted watermark image, W'.
6) Authenticate the digital signature shown in Fig. 3.

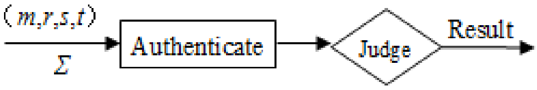


Fig. 3 Digital Signature Authenticate

IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

This paper has proposed a more secure image watermarking algorithm based on MECDH and AECDSA, the algorithm has been implemented in MATLAB R2012b with DSWT and SVD, calling *DLL* (Dynamic Linked Library) generated in Microsoft Visual Studio 2010 with MIRACL. The main results of our applications to the new algorithm are illustrated as follows:

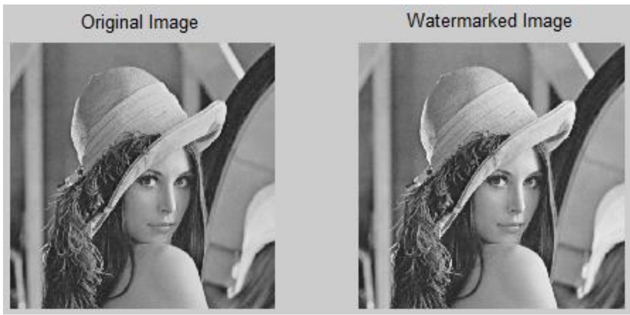


Fig. 4 (a) Original Image (b) Watermarked Image（σ=0.1, PSNR=45.17）

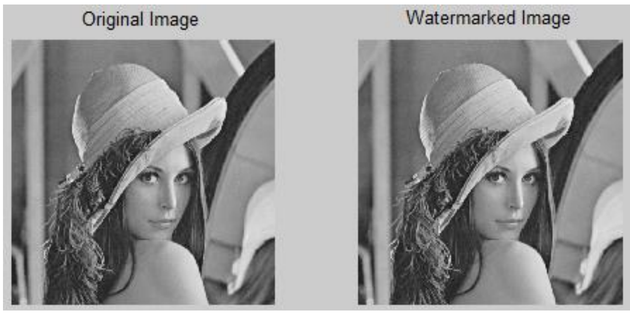


Fig. 5 (a) Original Image (b) Watermarked Image（σ=0.01, PSNR=64.80）

On the basis of the subjective evaluation, the original and watermarked images are shown in Fig. 4. Let us pay more attention to the objective evaluation criterion, PSNR, an approximation to human perception of reconstruction quality. A higher PSNR value normally means higher quality of reconstruction. The typical PSNR value for distorted images and videos are between 30 and 50 dB. Provided the bit depth is 8 bit, normally, the higher value of PSNR and the better performance for the algorithm.

Together with the subjective evaluation shown as Fig. 4&5, and PSNR values is 64.80 to 45.17 dB with σ∈(0.01,0.1), by which the invisibility of the final image embedded with the watermark image is effective, and the similarity of the original carrier image and the watermarked image is high. So the result of the proposed algorithm is more robust, more secure and better than that of [4] with 44.12 dB, [2] didn't mentioned it, but lower than the PSNR in [3] without professional and specific cryptography and digital signature technology.

In this paper, with the subjective evaluation shown as Fig. 6&7, the correlation coefficient between the original watermark image and the extracted one is 0.9974 to 0.9917, which means the close correlation between them. [2~4] didn't mention the corresponding data.

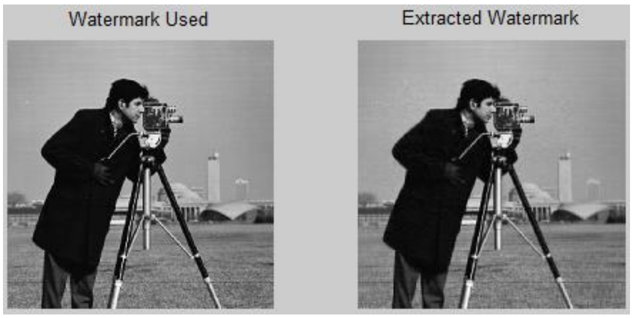


Fig. 5 (a) Original Watermark (b) Extracted Watermark（σ=0.1, correlation coefficient=0.9974）

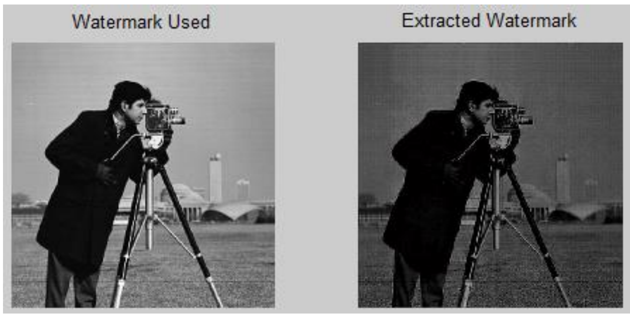


Fig. 6 (a) Original Watermark (b) Extracted Watermark（σ=0.01, correlation coefficient=0.9917）

To verify the robustness of the newly-proposed algorithm, we only test median-filtering attack and 45^{o}-rotation attack against the algorithm due to space limitations as Fig. 7. ~ 10. . The results of the algorithm have turned out to be robust despite some kinds of attacks.

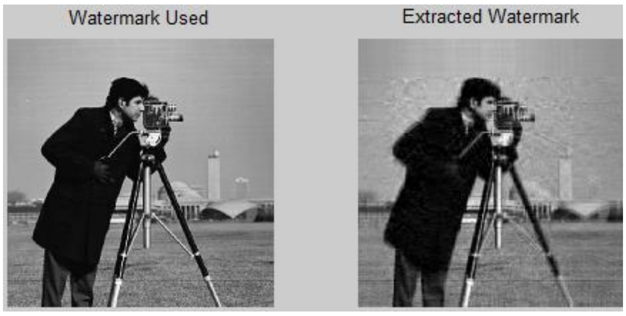


Fig. 7 Median-filtering Attack（σ=0.1, correlation coefficient=0.9748）
(a) Original Watermark (b) Extracted Watermark

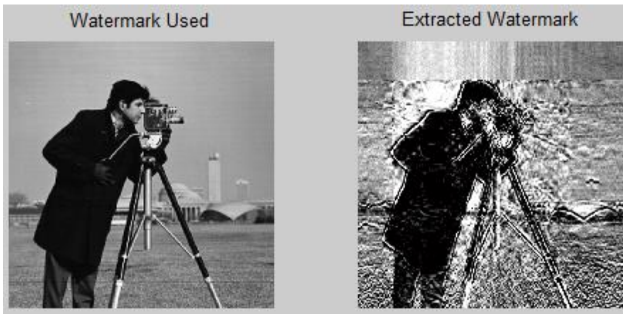


Fig. 8 Median-filtering Attack（σ=0.01, correlation coefficient=0.6134）
(a) Original Watermark (b) Extracted Watermark

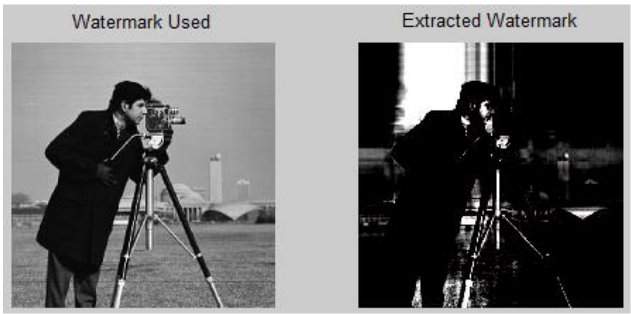


Fig. 9 45 ° -Rotation Attack（σ=0. 1, correlation coefficient=0.3724）
(a) Original Watermark (b) Extracted Watermark

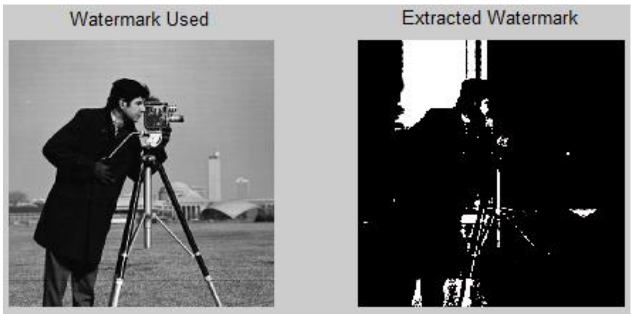


Fig. 10 45°-Rotation Attack（σ=0.01, correlation coefficient=0.3069）
(a) Original Watermark (b) Extracted Watermark

V. CONCLUSION

This paper presents a highly secure watermarking and digital signature authentication scheme with the improved MECDH and AECDSA algorithm running on MIRACL, which is implemented with DSWT and SVD. Both theoretical analyses and experimental results show that the proposed watermarking scheme with digital signature is more secure and efficient, authentic to protect digital copyrights, and is conforming to HVS with good invisibility and robustness. In next step we wish to implement quantitative analyses in the watermarking algorithm performances against all kinds of attacks, and to compute some elliptic curve with better performance over F_p.

REFERENCES

[1] D. Hankerson, A. Menezes, S. Vanstone, "APPENDIX B ECC Standards,", "Cryptographic Protocols," in *Guide to Elliptic Curve Cryptography*, New York: Springer, 2004, pp. 267–270. , pp. 153–204.

[2] Shalu Singh, Ranjan Kumar Arya, Harish Sharma, "Region based undetectable multiple image watermarking," in *ICCTICT*, 2016, pp. 141 -144.

[3] Ali Al-Haj, Noor Hussein, Gheith Abandah, "Combining cryptography and digital watermarking for secured transmission of medical images, " in *ICIM*, 2016, pp. 40-46.

[4] Milad Jafari Barani, Milad Yousefi Valandar, Peyman Ayubi, "A secure watermark embedding approach based on chaotic map for image tamper detection, " in *IKT*, 2015, pp. 1-5.

[5] Marco Indaco, Fabio Lauri, Andrea Miele, Pascal Trotta. "An Efficient Many-Core Architecture for Elliptic Curve Cryptography Security Assessment," in *FPL*, 2015, pp. 1-6.

[6] Songyuan Yan, "Public-Key Cryptography," in *Elliptic Curve*, CN:Dalian University of Technology Press, 2011, pp. 103-117.

[7] National Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-2, February 2000.

[8] Ali Makki Sagheer, "Elliptic Curves Cryptographic Techniques," in *ICSPCS*, 2012, pp. 1-7.

[9] Joseph H. Silverman, “Elliptic Curves over Finite Fields,” in *The Arithmetic of EllipticCurves*[M], New York:Springer-Verlag, 1986, pp. 130-145.

[10] Yong Ding, “Introduction to Elliptic Curve Cryptograpy,” in *Fast Algorithm Theory of Elliptic Curve Crytography*, CN:Post & Telecom Press, 2012, pp. 1-14.

[11] Tafta Zani, Ari Moesriami Barmawi, “Securing Elliptic Curve based El-Gamal against Pollard Rho attack using Elliptic Curve based Diffie-Hellman Key Exchange, ” in *ITST*, 2012, pp. 505-512.

[12] M.V. Tazebay and A.N. Akansu, “Adaptive Subband Transforms in Time-Frequency Excisers for DSSS Communications Systems, ” *IEEE Transaction on Signal Processing*, vol 43, no. 11, pp. 2776-2782, Nov. 1995.

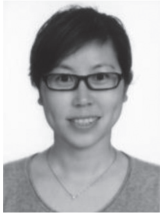
[13] Samira Lagzian, Mohsen Soryani, Mahmood Fathy. (2011, Mar.). “A New Robust Watermarking Scheme Based on RDWT-SVD: Embedding data in all subbands,” International Journal of Intelligent Information Processing, 2 (1), pp. 48-52.

[14] Paul Bao, Xiaohu Ma. (2005). “Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 15, no. 1, pp. 96-102.

Run Zhang is an associate professor of Computer Science at Communication University of China and a member of ACM. His research interests include Information Safety, Machine vision and Machine learning, etc. He has joined several National High Technology Research and Development Programs of China (863 Program) and published several theoretical technological articles.

Yong-Bin Wang is a professor of Computer Science and director of Science and Technology Office at Communication University of China. He is the director of Academic Committee at Key Laboratory of Vision-Audition Technology and Intelligent System, Ministry of Culture and Beijing Laboratory of Modern Performing Arts Technology. He is also a member of Beijing Committee of the Chinese People’s Political Consultative Conference. His research expertise is in the areas of media big data, social computing, and network new media. He gained 3rd class of S&T Achievements Granted with National Technology Invention Awards and 2nd class of Beijing Science and Technology Award. He has managed a variety research projects from Ministry of Science and Technology, Beijing Municipal Science & Technology commission. Prof. Yongbin Wang is the author of over 100 technical papers.

Jin-YaoYan received the B.S. degree from Tianjin University, the M.S. and Doctor (in engineering) degrees from Beijing Broadcasting Institute, the Ph.D (in science) degree from Swiss Federal Institute of Technology (ETH Zurich). Since 2010, he has been a Professor at Communication University of China, Beijing, P.R.China. He is a guest professor in communication system group at ETH Zurich. His research interests are in the areas of future network, multimedia communication, and cloud computing.



Shuang Feng is an associate professor of Computer Science at Communication University of China. Her research interests include Intelligence media processing, recommender systems and information retrieval. She joined the Department of Computer Science at the University of California, Santa Barbara as a visiting scholar in August 2013. She received her BSc and MSc from China Agriculture University, and her PhD from Communication University of China in 2013. She is a member of ACM. She managed more than 10 research projects from Ministry of Science and Technology, National High Technology Research and Development Program of China (863 Program), Beijing Municipal Science &Technology commission and obtained 2 national invention patents.