HAL
open science

Facial Identity Encryption with Kinoform and Phase-Key Watermarking for Homeland Security Agencies

Muhammad Naveed Iqbal Qureshi, Jin-Tae Kim, Sang-Woong Lee

To cite this version:

Muhammad Naveed Iqbal Qureshi, Jin-Tae Kim, Sang-Woong Lee. Facial Identity Encryption with Kinoform and Phase-Key Watermarking for Homeland Security Agencies. International Cross-Domain Conference and Workshop on Availability, Reliability, and Security (CD-ARES), Aug 2012, Prague, Czech Republic. pp.525-533, 10.1007/978-3-642-32498-7_40 . hal-01542453

HAL Id: hal-01542453

https://inria.hal.science/hal-01542453v1

Submitted on 19 Jun 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Facial Identity Encryption withKinoformand Phase-key WatermarkingforHomeland Security Agencies

Muhammad Naveed Iqbal Qureshi[1], Jin-Tae Kim[2,*], and Sang-Woong Lee[1,*]

[1] Computer Vision and Multimedia Laboratory, Department of Computer Engineering, Chosun University, Gwangju, 501-759, South Korea
[2] Laser Applications Laboratory, Department of Photonic Engineering, Chosun University, Gwangju, 501-759, South Korea
mniqureshi@hotmail.com, kimjt@chosun.ac.kr,swlee@chosun.ac.kr

Abstract. Internet has made it easy to access and transfercopyrighted material like facial ID to unauthorized users. In order to maintain confidentiality of any classified documents,especially, facial identity;their security and integrity are essential requirements for all law enforcement and homeland security agencies. We propose a new method to make the facial identity more secure and intact by usingencryptedkinoform facialidentity tags forsensitive image document such as passport,identitycard,security clearance gate passes, etc.Ourmethod to useencrypted phase-keywatermarking on the kinoformfacial identity- tags makes them more secure.

Keywords: Face Recognition, Kinoform, Optical Security, Image Encryption, Phase-key watermarking

1 Introduction

Document forgeries with false and duplicate facialidentity are big threats for any law enforcement agencies. Face recognitionsecurity systems are in market for more than half century.However, there is no absolutely secure and fail proof face recognition system developed up to date. The available systems mainly rely on computer vision based algorithms, such asprincipal component analysis, independent component analysis, linear discriminant analysis, evolutionary pursuit, elastic bunch graph matching, kernel method, trace transform, active appearance model,support vector machine, hidden Markov models and Bayesian framework, etc.

A Machine readable passport (MRP) system that usually installed on the immigration counter ofinternational airport useselectronic scanning techniques, particularly optical character recognition.

Most worldwide travel passports are MRPs with a special machine readable zone (MRZ), usually at the bottom of identity page at the beginning of a passport. The MRZ of passport spans of two lines and each line is 44 characters long. Following

* Corresponding Author

adfa, p. 1, 2011.
© Springer-Verlag Berlin Heidelberg 2011

information has to be provided in this zone: name, passport number,nationality, date of birth, sex, passport expiration date and personal identity number. There is aspace for optional, often country dependent and supplementary information[1].

A biometric passport known as an e-passport or digital passportcontain biometric information in an electronic chip.It is used to authenticate the identities of travelers. It uses contactless smart card technology including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or center page of the passport. The critical information is printed on the data page of the passport and stored in the chip. Public key infrastructure is used to authenticate the data which is stored electronically in the passport chip. The chip makes it expensive and difficult to forge when all security mechanisms are fully and correctly implemented [2].

Much remarkable work is already done in thefield of document security and authentication. However, we presentcombined approach of optics and computer vision toembed the encrypted kinoformfacial identityon next generation of passports, identity cards, security clearance passes and all the confidential imagedocuments that are sensitive in order to keep the homeland security intact.

A kinoform has inherent resistance against damage either natural or intentional, such as scratches and humidity. This feature makes its embeddingmore feasible on important documents.

2 Previous Work

In 1996,Stepien*et al.* proposed an idea about a distributed kinoform in optical security applications [3].That method was comprised on optically variable devices, diffraction and interference. Their work mainly relied on the use of very expensive and sophisticated optical equipment.

In 2003, Zhai *et al.*stated that non-cascade phase retrieval kinoform converges quickly and account for less data amount, which not only ensured good imperceptibility, but also reconstructed without conjugate images[4].

In 2003,Cable *et al.*stated anidea ofrecordingkinoformoptically generated hologram typically made on a photosensitive material by laser beams [5].Recorded kinoform images can be retrieved by a reconstruction beam.It isreconstructed optically to the original data through a Fourier transform lens.

In 2010,Hye *et al.* presented a technique for application of kinoform computer generated holograms (CGHs) to an identity tag system[6].Their idea comprehendedon 11-level kinoform CGH image generated on the tag sample by modified simulated annealing method at a low quantization error rate of 0.4% compared with the original data. In the retrieval process they used a commercial digital camera to take image of the kinoform ID tag. It is then reconstructed through computer to the original data with about 4 % reconstruction error rate.

In 2011, Deng*et al.*stated that kinoform accounts for much less data amount to be embedded than regular CGH[7].A kinoform can be extracted with only right phase key and right fractional order, and reconstructed to represent original watermark

without original cover image. They use random fractionalFourier transform in the kinoform generation process.

Optical reconstruction of kinoform can be easily explained by the following figure.

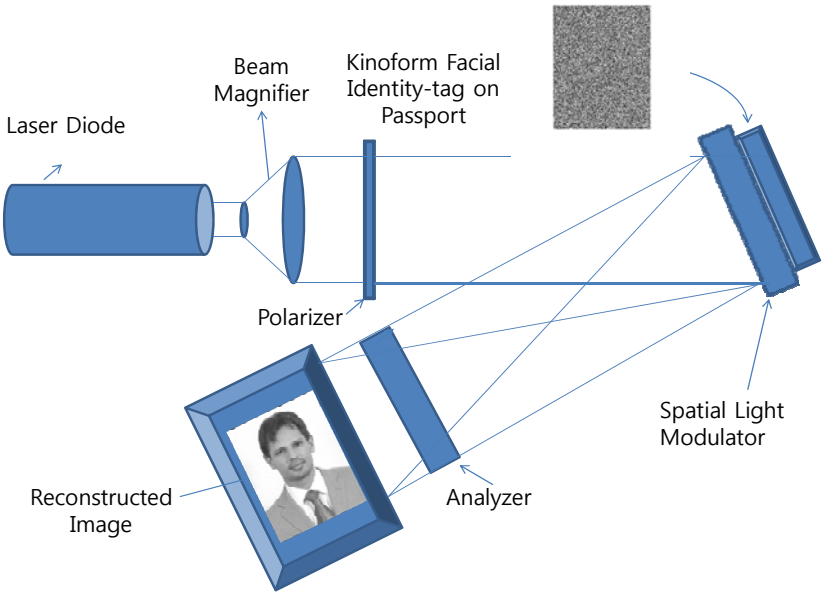

Fig.1. Electro-optical reconstruction of kinoform [9]

3 Robustness of Kinoform Identity-tag Against Natural and Intentional Damage

A kinoform is phase-only reference of input data and does not contain information about amplitude. We can suggest that these identity tags are more robust and damage tolerant than conventional identification tags. The kinoform can be reconstructed with high accuracy even if it is damaged by fire upto 50%, scratched or kept under extreme weather conditions such as rain or damp environment. Information in these identification tags is encoded in frequency domain. Watermarking is done in spatial domain. Collectively our identification tag is more robust as compared to other secure identification-tags such as barcodes, etc.

Robustness of kinoform had been investigated and proved in the work of Hye *et al.* [6]. According to them, even if we lose 50 % of the entire kinoform identity-tag, we can reconstruct the original identity with 12.5% error.They used kinoform (CGH) tags in which one has 25% damage, and the other has 50% damagephysically. Both tags were detected optically and recovered on the same condition, have the same lightintensity, the same camera angle, and so on. The recovered data were compared in terms of error rateswith the original data.

We propose to use kinoform instead of facial identity. It makes the document more robust against damage and corruption. If, in case of scratch or fire we lose 50 % of the entire identity tag, we can recover the original identity from it with a maximum error of 13 %.

Following are the experimental results of reconstruction with 50% of data loss on kinoform identity tag. We can easily verify the facial identity with the reconstructed image.

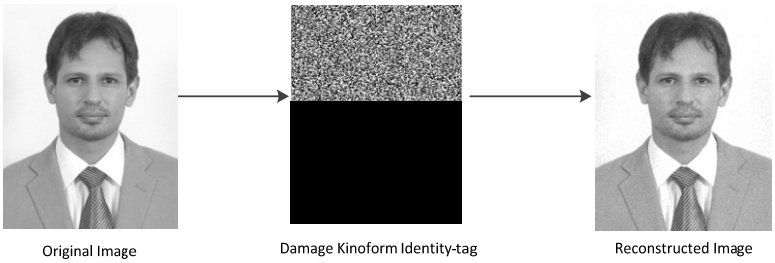

Fig.2. Original input data and its reconstructed data for a facial identity kinoform tag with 50% damage

Fig. 2shows that the facial identity kinoform reconstructs of original data at an errorrate of 13% for the 50% tag loss in the experiments.

4 Overview of Proposed System

We propose a method of making travel document like a passport safer than earlier from forgery. Kinoform facial identity-tags are impossible to reconstruct and fabricate without knowledge of actual identity and exact phase-key as well as the complex optical phenomenon details. Without highlynormalized cross correlation value, original information cannot be retrieved from the kinoform identity tag unless we know the exact phase key.

5 Construction of Kinoform Identity-tag

We construct kinoform identity tag of the facial identity photograph by optical instruments. After optical construction, we took a photograph of the kinoform of the object with an ordinary digital camera. We do Encryption of the phase-key by using substitution cipher databasein next step.Then byusing least significant bit method ofwatermarking, wehidephase-key along-with error correcting codes in kinoform identity tag. We do watermarking with standard image processing tools. After watermarking, our encrypted kinoform facial identity tag becomes ready to be printed on passport.

Fig.3 describes our proposed system and workflow stepwise for the construction of encryptedphase-key watermarked kinoform facial identification tags.

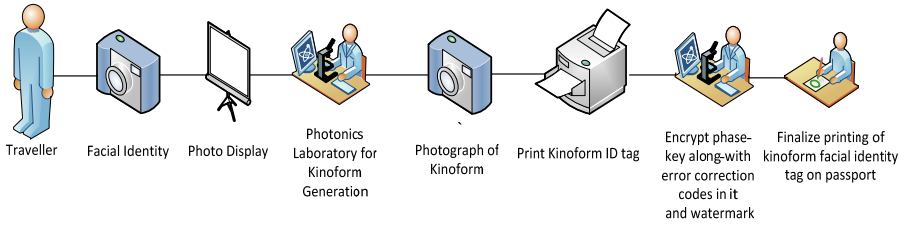

Fig.3. Kinoform facial identity tag generation process

In rest of the section 5 we will discuss each step of the Kinoform construction process in more detail.

5.1 *Kinoform*

A phase-only reference-less optically generated Fourier hologram, which gives a nonsymmetrical image in the reconstruction process, is known as kinoform [3]. Although it can be generated by CGH method but we used optical instruments for its construction. Kinoform is a phase only optical element and its amplitude should either bekept constant or unity.In reconstructionif we use only phase information of kinoform of the inputimage, it may contain noise because of the amplitudenegligence.The kinoform is designed in such a manner that maximum phase modulation of the incident light is2**π.**

Our idea is to embed encrypted watermark of person specific phase information in the face image kinoform.

Fig.4. Facial identity photograph and its correspondingkinoform identity tag developed in our photonic engineering laboratory

5.2 *Watermarking*

From previous works in the field of watermarking we already know that size of secret message should not exceed more than 25% of cover image. If we hide only encrypted phase-key information in the cover image, we can avoid this limit violation.

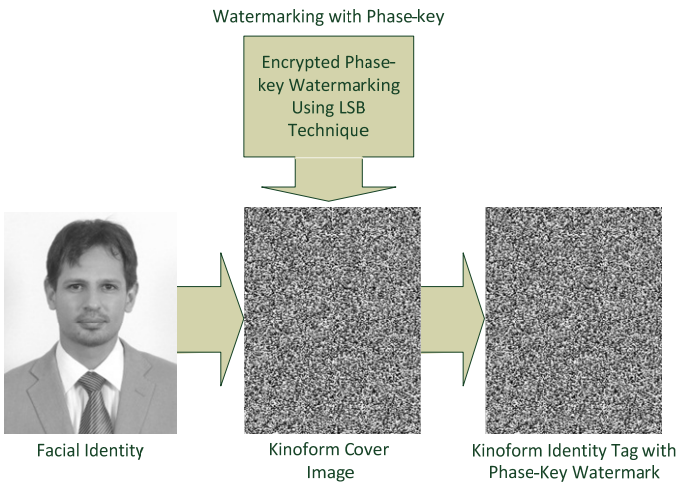

Fig.5. Our proposed idea to generate kinoform facial identity tag with phase-key watermarking

In 2000 Chang and Orchard stated that a watermarking scheme has two operations; engravingand detection[8]. It is convenient to represent these two operationsas two subsets in the image space, the Kernel Kand the set of watermarked images W. Given the originalimage I, engraving embeds a watermark into an image I, resultingin another image I', which is the image in K closest to I.The detection takes an image I' and declares it to be watermarkedif and only if I' belongs to W.

We propose to use least significant bit (LSB) watermarking technique to hide the phase-key inside the cover image. The cover image is itself a secure identity because it is a kinoform of original facial identity and it cannot be reconstructed easily. Fig. 5 describes this phenomenon.

Phase-key encryption adds another fold of security to the identity-tag. It is described in detail in the following sub-section.

5.3 Phase-key Encryption

To enhance the security of kinoform identity-tag, we propose to embed another fold of safety by using substitution cipher encrypted phase-key as a watermark instead of the original phase-key.

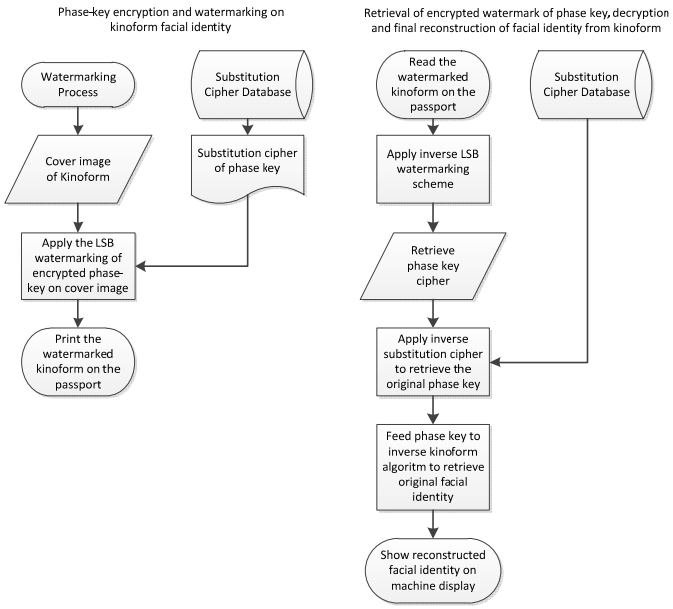

Fig.6. Process of encryption and decryption of phase-key watermarking

Database of substitution cipher should be kept as a top secret material under surveillance of government agencies to make this scheme more reliable and secure. The same reference database of substitution cipher should be embedded in the memory of passport reading device for reconstruction of original facial identity. Since the passport reading devices are only available at the immigration counters of airport under strict surveillance, we can assume that it is safe to embed the substitution cipher database in their memory.Fig.6explains this encrypted watermarking process stepwise both at the construction and reconstruction phases.

6 Reconstruction of Facial Identity from Kinoform Identity-tag

In the reconstruction process of encrypted kinoform identity-tag, device should work in the following steps:

- Read the encrypted kinoform facial identity-tag on passport
- Retrieve phase-key watermark from kinoform identity-tag
- Decrypt phase-key with substitution cipher embedded in the memory of reading device
- Check phase-key for errors by using the error correcting algorithm

Reading machine will run error correction algorithmto make phase-key retrieval process more reliable.

After retrieving the correct phase key our facial identity reconstruction device will supply it to inverse kinoformgenerationalgorithm.We propose to use function of inverse fractional Fourier transformwith the correct decryptedphase key which is retrieved and decrypted from the watermark.

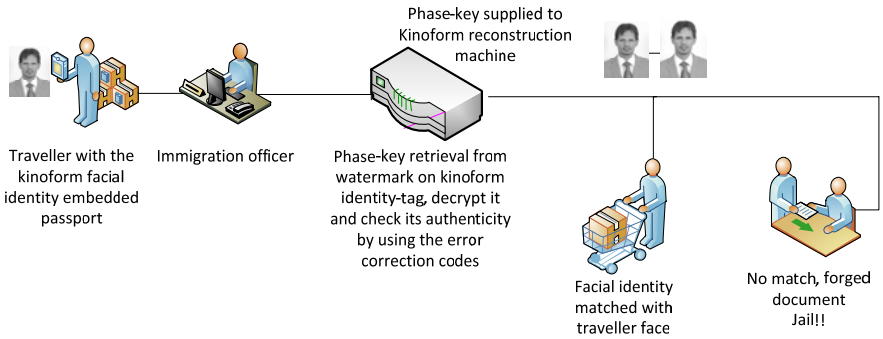

Fig.7. Reconstruction of facial identity from kinoformtag at airport immigration counters

Since in the construction of Kinoform we only preserve the phase information and make the amplitude of source object either as a constant or unity, we do not need to care about amplitude information at the reconstruction.

We do not need much processing power for computinginverse fractionalFourier transform of the kinoform. The whole reconstruction algorithm can be easily embedded in 32-bit SoC for digital image and signal processing.

7 Conclusion and Future Work

We can claim that this technique is very secure because once the kinoform is watermarked with the encrypted phase key; it cannot be reconstructed by optical instruments. If we try to reconstruct it with optical instrumentation, only noise will be generated in result. It is impossible to retrieve the phase-key watermark by any optical process. Moreover, the substitution cipher is another fold of security that we have embedded in encryption of phase-key watermarking on kinoform identity-tag. Our proposed reconstruction method is the only way to reconstruct original facial identity.

The idea of kinoform based facial identity tag implementation can effectively reduce the documentforgery.This system has 3-fold security and this feature makes it almost absolutely secure. We have seen that the reconstruction of original data is impossible without original phase key information. Evenif the phase key is extracted from the watermark, it is not very easy to decrypt it.Reconstruction of the original facial identity image from the kinoform identity tag is extremely difficult unless we do know the exact reconstruction algorithm.

This idea can be implemented on any image document. We can further conclude that kinoform based security solutions are much better and more secure as compared to the conventional identity-tag verification systems.

Acknowledgement

This work was supported by the National ResearchFoundation of Korea(NRF) grant funded by the Korea government(MEST)(no.2009-0075968).

References

1. Machine readable passport http://en.wikipedia.org/wiki/Machine-readable_passport.
2. Biometric passport http://en.wikipedia.org/wiki/Biometric_passport.
3. PawelStepien, RemigiuszGajda, and Tomasz Szoplik: Distributed Kinoform in optical security applications: Optical. Engineering**35**, pp. 2453-2458,1996.
4. HongchenZhaia, FuminLiua,Xiaoping Yanga, GuoguangMua,and Pierre Chavel: Improving binary images reconstructed from Kinoform by amplitude adjustment: Optical Communication**219**,pp. 81–85,2003.
5. Adrain Cable, Peter Mesh, and Timothy Wilkinson: Production of computer-generated holograms on recordable compact disc mediausing a compact disk writer: Optical Engineering**42**, pp. 2514–2520, 2003.
6. Hye-Rim Kim, Ki-Mun Pak, Ki-Woo Jun, Hyun-Whan Choi,Ji-Song Lim,and Yong-Hyub Won:Application of Kinoform CGHs to an IDTag System: IEEEPhotonics Journal, pp. 553 – 562,2010.
7. Ke Deng, Guanglin Yang, and Haiyan Xie: A blind robust watermarking scheme with non-cascade iterative encrypted kinoform: Optical Express **19**, 10241-10251, 2011.
8. Ee-Chien Chang andMichaleOrchard: Geometric properties of watermarking schemes:Proceedings International Conference on Image Processing**3,** pp. 714-717, 2000.
9. HuadongZheng,Yingjie Yu, HaiyanQian, andAnandAsundi: Reduction of speckle noise by multi-kinoform in holographic three-dimensional display:Proceedings of Ninth International Symposium on Laser Metrology, pp. 7155- 7155,2008.