©2016 Society for Imaging Science and Technology
DOI: 10.2352/ISSN.2470-1173.2016.8.MWSF-084

Security Evaluation based on the Analytic Hierarchy Process for First-line Anti-counterfeit Elements

Manabu Yamakoshi, Junichi Tanaka, Hiroshi Iwasaki; Research Institute, National Printing Bureau of Japan; Odawara, Kanagawa /Japan

Abstract

First-line security features such as intaglio latent printing and watermarks for security documents play a very important role in combating counterfeiters. Against such a background, the derivation of criteria for the evaluation of security elements and the practice of such evaluation are critical processes in security improvement. Although methods of determining the quantitative value security of DOVIDs in first inspections have been examined in previous work, further study is needed to address issues with limitations on targets of evaluation, a lack of clarity in evaluation scales for measurement corresponding to individual criteria, and uncertainties in MDA methodologies. The authors previously established a method to support quantitative security evaluation for elements in first-line inspections for security documents. In the study reported here, a security criteria evaluation tree for general elements was first derived. The tree was then used to develop a set of security evaluation tools in spreadsheet software based on the analytic hierarchy process. Security features were quantitatively evaluated, and the scores obtained were visualized as security profiles. The results helped to clarify individual characteristics, including security weaknesses in elements, and approaches for the selection of suitable elements for implementation in products.

Introduction

Counterfeiting and alteration threats to security documents such as banknotes, e-Passports and postal stamps are serious social issues. Despite work on the development of a new counterfeit deterrent system incorporating artifact-metrics [1] and PUFs [2] [3] using information technologies for security documents, first-line security features [4] still play a very important role in combating counterfeiters. Such features, including intaglio latent printing and Optical Variable Inks (OVI), are developed for human inspection based largely on the senses of sight and touch. They provide the significant advantages of convenience and intuitiveness without the need for related equipment in authentication. Accordingly, the derivation of criteria for the evaluation of security elements and the practice of such evaluation are critical processes in security improvement.

A preceding report [5] proposed a method for evaluation of the quantitative value security of DOVID elements such as holograms using multi-criteria decision analysis with a set of security criteria. However, issues still requiring attention include limitations on targets of evaluation, a lack of clarity in evaluation scales for measurement corresponding to individual criteria, and uncertainties in MDA methodologies.

Purpose

The study's objective was to establish a method for quantitative evaluation of security elements such as intaglio latent images, OVIs and holograms, which are typical counterfeit deterrence features for first-line inspection in banknotes, passports and other security documents. To this end, the authors first derived a security criteria evaluation tree for general first-line elements including DOVIDs. The tree was then used to develop a set of security evaluation tools in spreadsheet software based on the analytic hierarchy process (AHP). These tools were subsequently used for trial security evaluation of intaglio latent images, OVIs and holograms. Vulnerabilities in the visualized security profiles and related improvements were also discussed.

Method

Derivation of evaluation tree for security elements

The leading set of security criteria was based on a tree system approach. The crucial advantages of this process are efficiency and the elimination of leaks/overlaps in criteria. The research team consisted of four experts with backgrounds in security evaluation, element identification, material development and human ergonomics. The definition of security criteria and terminology relating to measures against counterfeiting were brainstormed to ensure full consensus within the team. An overview of the security class evaluation tree is shown in Figure 1.

The following preconditions were applied to team discussions.

- The four basic classes of security, usability, social acceptance and cost are required as general criteria for elements. However, these are interrelated rather than being entirely independent. By way of example, higher cost is associated with improved security, and higher usability is associated with increased social acceptance.
- Sub-sets (layers) of all classes should be as independent as possible from other criteria.
- The targets of evaluation are security elements classified for first-line inspection in the security class.

Security tree terminology

Some technical terms in this paper have meanings extending beyond the scope of general usage. The research team introduced concept arrangements for counterfeit risks and the deterrent system with reference to previous [6] and technical standards [7] [8]. Some important and uncommon terms relating to security criteria are listed below by tree level.

Level 1 criteria

1. *Authenticity*: term relating to the characteristic of being genuine and recognizable as real
2. *Inspection*: term relating to the process of authentication.
3. *Anti-reverse engineering*: term relating to the difficulty of clarifying the principle and mechanism behind a security element
4. *Integrity*: term relating to the soundness of an element without tampering, transplantation and informational inconsistency among security elements

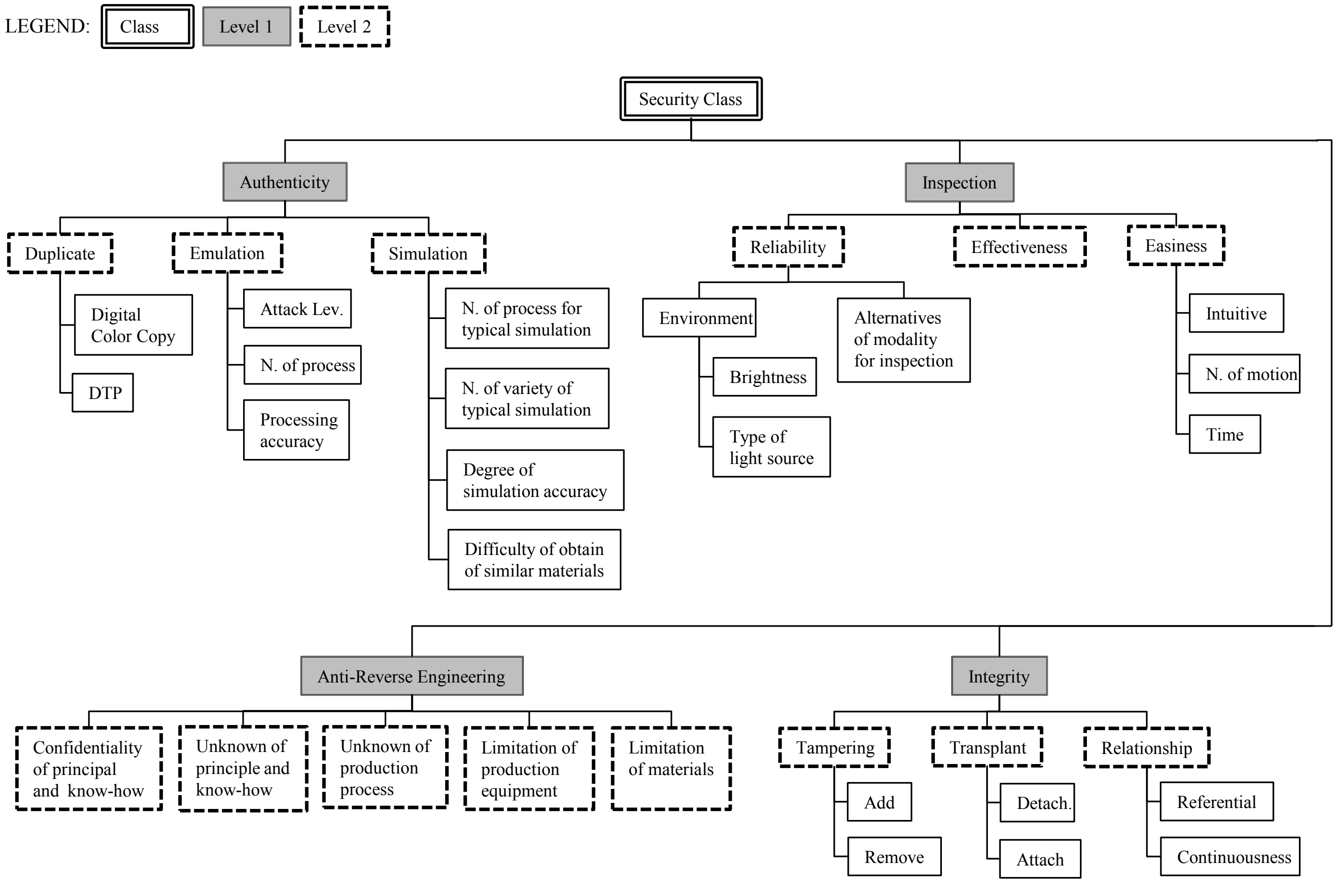


Figure 1. Overview of the security class evaluation tree

Level 2 criteria:

5. *Duplication*: reproduction of an original using a photo scanning device or other technology
6. *Emulation*: reproduction of an original intended to pass close scrutiny by a qualified examiner
7. *Simulation*: imitation of an original in a form intended to pass as genuine in ordinary use
8. *Reliability*: trustworthiness for adequate performance over the intended lifespan under expected conditions
9. *Effectiveness*: certainty of authentication
10. *Relationship*: informational inconsistency and physical overlap of elements

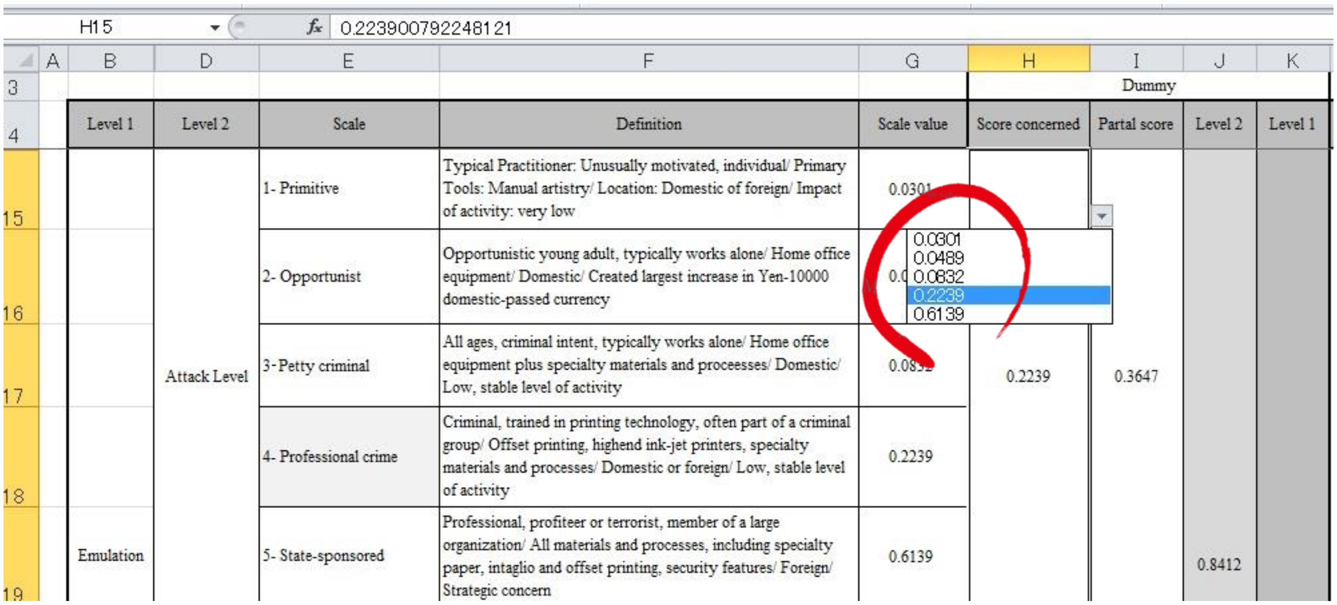
Detailed criteria:

11. *DTP*: resilience to reproduction by desktop publishing
12. *Attack level*: primitive, opportunist, petty criminal, professional criminal and state-sponsored (5 levels based on counterfeiter resources)
13. *Number of processes*: number of processes necessary to implement an element in consideration of the lead time
14. *Number of typical simulation varieties*: number of typical simulation types as determined from thought experiment
15. *Degree of simulation accuracy*: estimated level of elaboration in simulation as determined from thought experiment
16. *Difficulty of obtaining of similar materials*: metric based on obstacles to the procurement of similar materials (rather than original materials) in consideration of the risk of simulation
17. *Number of operations*: number of operations necessary for authentication including tactile sensation, tilting and visual inspection against a light source
18. *Addition*: difficulty of adding new printing patterns, implemented artwork and other visuals
19. *Removal*: difficulty of removing printing patterns, artwork and other visuals
20. *Detachment*: difficulty of detaching an element from the substrate
21. *Attachment*: difficulty of mounting an element detached from others
22. *Reference*: possibility of informational inconsistency based on inquiry in relation to other elements
23. *Continuousness*: possibility of attribution analysis based on overlap or concord of other elements.

Evaluation scales

Evaluation scales corresponding to each criterion were also defined. The scales differed for individual criteria in consideration of their characteristics. Some had either two results (pass or fail) or five (Excellent > Good > Fair > Poor > None), some were quantitative (such as one expressing processing accuracy with values between 10 and 50 um), and others were quantitative. By way of example, the elements in the “Secrecy of principle and know-how” scale are listed below.

DOI: 10.2352/ISSN.2470-1173.2016.8.MWSF-084



H15 *fx* 0.223900792248121

	A	B	D	E	F	G	H	I	J	K
3							Dummy			
4		Level 1	Level 2	Scale	Definition	Scale value	Score concerned	Partal score	Level 2	Level 1
15			Attack Level	1- Primitive	Typical Practitioner: Unusually motivated, individual/ Primary Tools: Manual artistry/ Location: Domestic of foreign/ Impact of activity: very low	0.0301	0.2239	0.3647	0.8412	
16				2- Opportunist	Opportunistic young adult, typically works alone/ Home office equipment/ Domestic/ Created largest increase in Yen-10000 domestic-passed currency	0.0				
17				3- Petty criminal	All ages, criminal intent, typically works alone/ Home office equipment plus specialty materials and proceesses/ Domestic/ Low, stable level of activity	0.0832				
18				4- Professional crime	Criminal, trained in printing technology, often part of a criminal group/ Offset printing, highend ink-jet printers, specialty materials and processes/ Domestic or foreign/ Low, stable level of activity	0.2239				
19		Emulation		5- State-sponsored	Professional, profiteer or terrorist, member of a large organization/ All materials and processes, including specialty paper, intaglio and offset printing, security features/ Foreign/ Strategic concern	0.6139				

Figure 2. Evaluation tool interface: "Attack level" includes 5 scales. Definition of each scale was referring to [9].

- Compulsory education
- Higher education
- Printing expertise
- Knowledge of security printing, including hacking information

It should be noted that open discussion of detailed scales fears to result in security degradation for some elements.

Development of evaluation tools based on AHP methodology

Analytic hierarchy process

The analytic hierarchy process allows users to intuitively assess the relative weight of multiple criteria (or multiple alternatives against a given criterion). Its major innovation is the introduction of pairwise comparisons as a method based on research showing that humans are adept at recognizing whether one criterion is more important than another even when quantitative ratings are unavailable.

Suppose A_1, A_2, A_3,…, A_m be set of stimuli. The quantified judgments on pairs of stimuli A_i and A_j are represented by m-by-m matrix A. m is the number of criteria and need to be under seven. If m is over seven, quantified judgments can't be assured.

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{im} \\ \vdots & & \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mj} & \cdots & a_{mm} \end{bmatrix} \tag{1}$$

Here, importance of a_i comparing a_j defined as a_{ij}. As well, importance of a_j comparing a_i represents a_{ji}. They are defined as inverse number. Also, the all value of on-diagonal elements a_{11},…, a_{ij},…, a_{mm} are one.

Next, w_i (i = 1,…, m), the set of numerical weights of m number of criteria are calculated based on principal eigenvalue method.

In matrix A, λ and q (q_1,…, q_m) *which* satisfies the equation (2) are determined.

$$\boldsymbol{Aq} = \lambda \boldsymbol{q} \tag{2}$$

$$\begin{bmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{im} \\ \vdots & & \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mj} & \cdots & a_{mm} \end{bmatrix} \begin{bmatrix} q_1 \\ \vdots \\ q_i \\ \vdots \\ q_m \end{bmatrix} = \lambda \begin{bmatrix} q_1 \\ \vdots \\ q_i \\ \vdots \\ q_m \end{bmatrix} \tag{3}$$

Where, λ is eigenvalue and q is eigenvector of matrix A.

In m-by-m matrix A, eigenvalue λ which satisfies equation (2) exist at most m. The maximum λ represents λ_{max} ($\lambda_{max} \neq 0$). In eigenvector method, each element of matrix A is described with ratio of eigenvector corresponded to λ_{max}.

$$a_{ij} = \frac{q_i}{q_j} \tag{4}$$

Finally, w_i (i = 1,…, m), the set of numerical weights for m criteria can be regarded as elements of the eigenvector q corresponded to maximum eigenvalue λ.

In addition, validity of w_i (i = 1,…, m) can be verified with *Consistency Index* (*C. I.*) (5).

$$C.I. = \frac{\lambda_{\max} - m}{m-1} \tag{5}$$

To assure of validity of w_i, the *C. I.* is desirably approximately 0.150 or less [10]. If *C. I.* is over 0.150, pairwise comparisons should be executed again.

Evaluation tools

Based on the evaluation tree derived in the study, the evaluation process with AHP was implemented in a spreadsheet environment. Figure 2 shows some of the tools used. The total

©2016 Society for Imaging Science and Technology
DOI: 10.2352/ISSN.2470-1173.2016.8.MWSF-084

security class score for elements can be calculated and the security profile can be visualized simply by inputting suitable scale values as listed in the red-circled pull-down menu in the figure.

Experiments

Preparations

Before the trial evaluation, scale values and evaluation scenarios were set based on brainstorming among the four experts.

- Calculation of scale value sets corresponding to individual evaluation criteria

The values were defined as eigenvectors based on a pairwise comparison matrix for the evaluation scale.

- Setting of evaluation scenarios denoting criterion priority

The values were defined as eigenvectors based on a pairwise comparison matrix (Table 1) for criteria under each layer of the tree. Several scenarios were defined with particular criteria emphasized in addition to the assumed ideal standard (Figure 3).

Table 1. Pairwise comparison matrix for the standard scenario of Level 1

	Authenticity	Inspection	Rev. Eng.	Integrity	Wt.
Authenticity	1	3	4	5	0.5266
Inspection	1/3	1	3	5	0.2786
Rev. Eng.	1/4	1/3	1	3	0.1307
Integrity	1/5	1/5	1/3	1	0.0642

(C.I. = 0.0631)

1 = NA (Equal)	
3 = Slightly important	1/3 = Slightly unimportant
5 = Inportant	1/5 = Uninportant
7 = Very important	1/7 = Very unimportant
9 = Extreamly inportant	1/9 = Extreamly uninportant

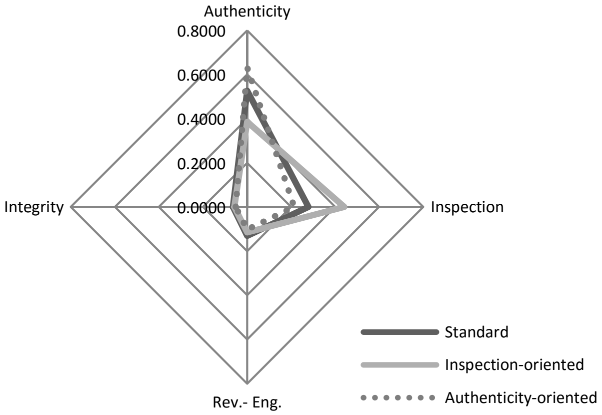


Figure 3. 3 types of evaluation scenarios for level 1

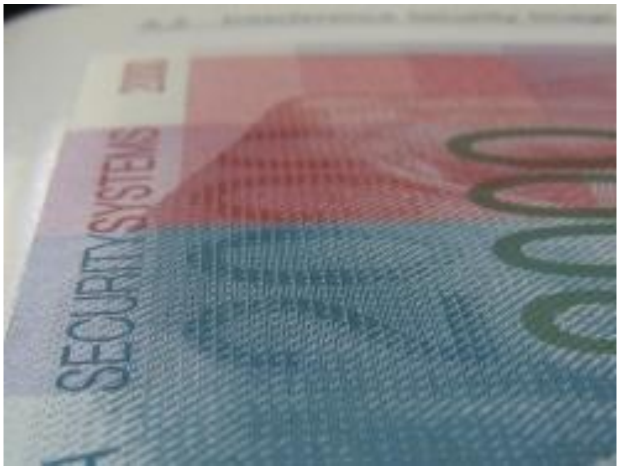


Figure 4. Intaglio latent image: Visible if the note is viewed at an oblique angle. The number 2000 appears in a light shade (viewing along the width of the note) or dark shade (viewing along the height of the note)

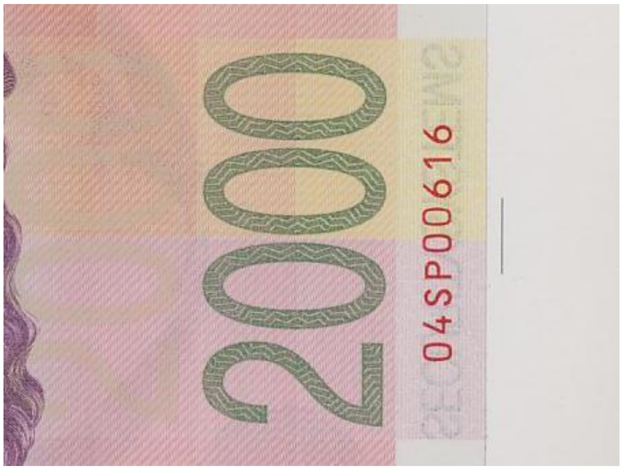


Figure 5. OVI intaglio: The number 2000 changes color from green to blue with increasing angle of observation. Apart from the color change, security is reinforced by intaglio printing.

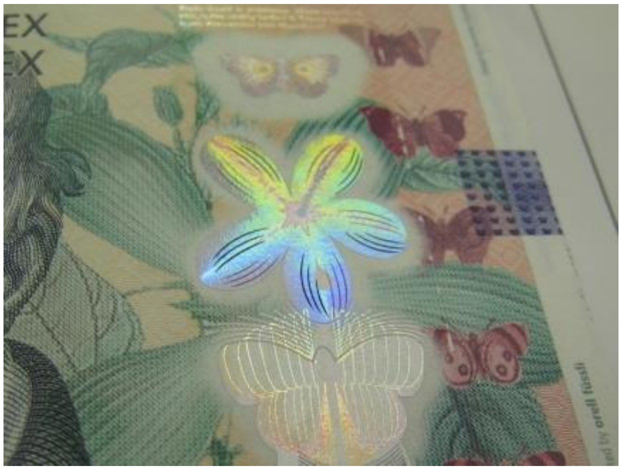


Figure 6. Hologram (OVD-stripe): The diffractive features of the foil stripe are applied in registered with the print of the banknote, thereby enabling unique synergies between the OVD foil and the overprinting as well as printed background.

Trial evaluation

AHP absolute measurement method is adopted for evaluation in this paper. The measurement score V (0 ~ 1) of a criterion is calculated the equation (6).

$$V = \frac{q_i}{p_{max}} \tag{6}$$

where, q_i is the level applicable of w_i, and p_{max} is maximum eigenvector of q_i.

The element evaluation targets classified as first-line anti-counterfeit features were an intaglio latent image (Figure 4), an OVI intaglio (Figure 5) and a hologram (Figure 6). All real elements are included in [4]. Scores were given for every criterion and layer using the evaluation tools with full consensus among the research team. The total security class score for each element was integrated with all partial scores in sub-layers.

Results and discussion

Evaluation results for the three evaluation scenario types are shown in Figure 7. The hologram exhibits the best performance. The score difference is the most noticeable on inspection- oriented scenarios, since hologram has some advantage of inspection criterion comparing other elements.

The security profiles of level two for the three elements are shown in Figure 8. The highest total score for the hologram is partly attributable to the superiority of emulation, the easiness for inspection, secrecy of the principle, and the material. Especially, easiness of inspection is noteworthy. Attractiveness for human eye and flashy changes of image are important characteristics for first-line inspection element. On the other hand, there is inferiority of tampering and transplant for the hologram. As for countermeasures, overlapping with prints including intaglio and fine complicated patterns by de-metalized should be implicated on hologram.

The scores of simulation and principal which is one of the subset of anti-reverse engineering are low for all elements. It is the essential issue for the first-line security elements as long as the judgment depends on vague human sense. To solve the issue two strategies are proposed. One is the effective user education for handle security elements adequately to avoid false acceptance of simulation. The other is introducing a new profound principle to elements, which makes it difficult to forge by counterfeiters.

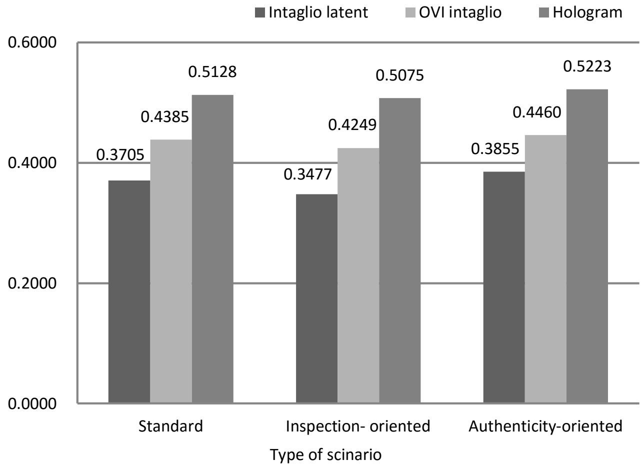


Figure 7.Security total scores by 3 type of scenario

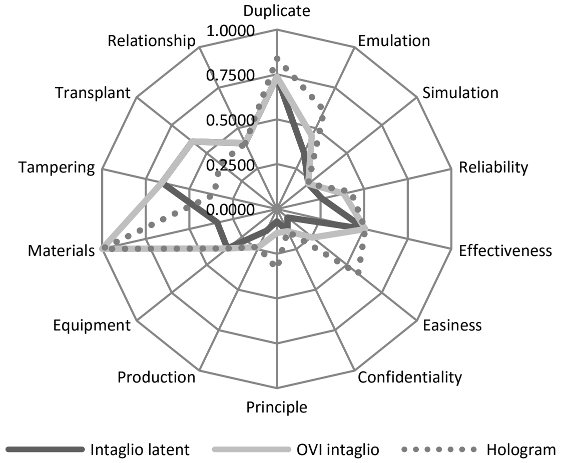


Figure 8.Security profiles of level two for three elements

Summary

The authors established an elaborate evaluation tree for general security elements in first-line inspections and defined suitable scales for measurement corresponding to each criterion. Using AHP methodology, evaluation scenarios and scale values for each criterion were set to enable scoring. These achievements contribute to improved accuracy in evaluation for security elements.

The tools developed in the study were used to evaluate intaglio latent image, OVI intaglio and hologram. Principles, materials and manufacturing processes differ among these elements, but the evaluation results highlighted their individual characteristics in the form of security profiles. These profiles also help to highlight security weaknesses and support the selection of suitable elements for product implementation.

Matters to be addressed in future work include evaluation of overall performance in all classes (including usability, social acceptance and cost) and security evaluation for whole products rather than single elements.

Acknowledgements

The authors wish to acknowledge Dr. Tsutomu Matsumoto of the Graduate School of Environment and Information Sciences at Yokohama National University for his input, which included reviewing the tree's architecture and the scale's validity as well as suggesting the need to hold open discussions on document security beyond secrecy toward standardization.

References

[1] M. Yamakoshi, J. Tanaka, M. Furuie, M. Hirabayashi, T. Matsumoto, "Individuality evaluation for paper based artifact-metrics using transmitted light image," Proc. SPIE 6819, 68190H, 2008.

[2] Pappu, Ravikanth, "Physical One-Way Functions," Ph.D. thesis, Massachusetts Institute of Technology, 2001.

[3] Guajardo, Jorge, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," Proceedings of CHES 2007, LNCS 4727, Springer-Verlag, pp. 63–80, 2007

DOI: 10.2352/ISSN.2470-1173.2016.8.MWSF-084

[4] Rudolf L. van Renesse, "Optical Document Security," Third Edition, Artech House, ISBN 1-58053-258-6, 2005.

[5] Ana A. Andrade and Jose M. Rebordao, "Evaluation of DOVID security under 1st line inspection," SPIE Vol. 4677, 2002

[6] Hans de Heij, "Innovative approaches to the selection of banknote security features" Banknotes of the World, Issue #8 and #9, Inter Crim Press, Moscow, 2010

[7] ASTM, F1448 – 93a, "Standard Guide for Selection of Security Technology for Protection Against Counterfeiting, Alteration, Diversion, Duplication, Simulation, and Substitution (CADDSS) of Products or Documents," 2006.

[8] ISO 12931, 2012, "Performance criteria for authentication solutions for anti-counterfeiting in the field of material goods," 2012.

[9] Committee on Technologies to Deter Currency Counterfeiting, National Research Council, "A Path to the Next Generation of U.S. Banknotes : Keeping Them Real," The National Academies Press, 2007

[10] Saaty, Thomas L. Multicriteria Decision Making - The Analytic Hierarchy Process, Pittsburgh, RWS Publications, 1992.

Author Biography

Manabu Yamakoshi received a BS in engineering from Chiba University in 1990 before working at the Research Institute of Japan's National Printing Bureau and focusing on the development of security elements, banknote security evaluation and standardization issues relating to e-passports. He served as a research professor at Cal Poly San Luis Obispo from 2008 to 2010 and received a PhD in engineering from Yokohama National University in 2011. He is a committee member of ISO/IEC JTC1/SC17.