# Security design of valuable documents and products

Rudolf L. van Renesse

**Conference on Optical Security and Counterfeit Deterrence Techniques**
San José, California, USA
January 28 – February 2, 1996
SPIE vol. 2659, pp. 10 – 27

VanRenesse Consulting
Willem de Zwijgerlaan 5
2582 ED The Hague
The Netherlands
Phone +31 70 3540 333
Email ruud_van_renesse@zonnet.nl

# Security design of valuable documents and products

Rudolf L. van Renesse*


## ABSTRACT

A method of security design is presented, founded on a systematic seven step approach: (1) drafting a security policy, (2) a list of requirements, (3) a security scheme and (4) a fraud-risk analysis. Based on these documents the security measures can be selected (5) and implemented (6), to result in a security product (7). Simulation and/or experiments are required to assess the relevant properties of the design or product. The actual evaluation consists of comparing these properties with the requirements. Subsequently weak and strong points, and possible paths of attack will be established. In case the evaluation reveals a considerable mismatch between requirements and characteristics, the design cycle has to be passed through again and either the requirements must be adapted, the design or both. This procedure is repeated until the remaining mismatch between requirements and design properties becomes acceptable. It is paramount that an evaluation is not postponed until the final stage of product realisation, but is carried out in the early phases of the project. In fact, it is beneficial if all seven steps of the design are the subject of an evaluation. Some design considerations for optically variable devices will be discussed.


**Keywords**: security design and evaluation, statement of requirements, fraud-risk analysis, optically variable device

## 1. INTRODUCTION

Each design, whether that of a walking stick, a coffee mill or a security product, stems from a problem. The existence of a problem as such however does not suffice. The party concerned must develop awareness of the problem and must consider it of sufficient importance to justify creative action.

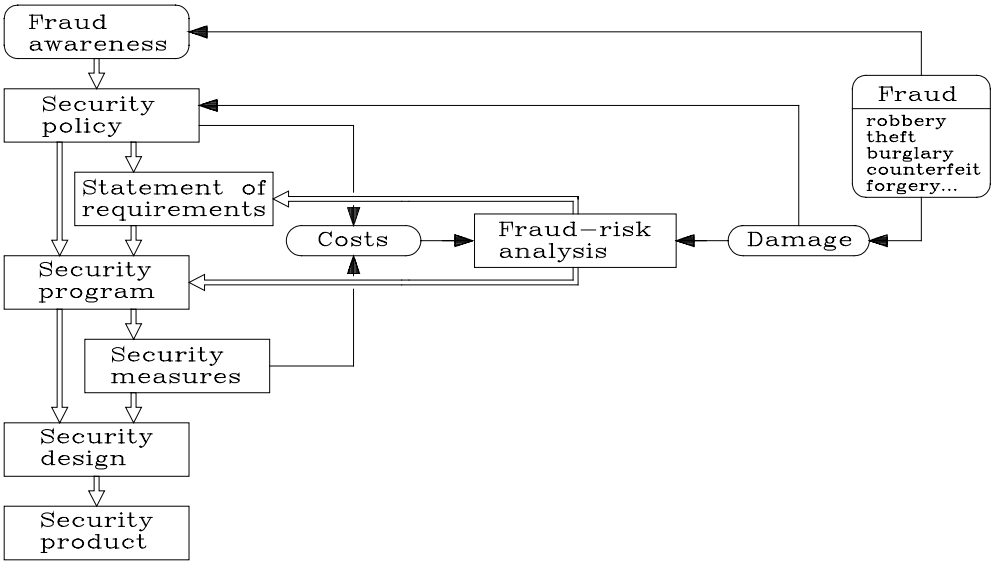


**Figure 1** - The development of a security product (after [1]).

Ideally, the development of a security product passes, in a systematic manner, through several steps: from the awareness of a security problem (e.g. fraud awareness), via analysis of the problem and the subsequent design steps to the final product. These subsequent steps are represented schematically in figure 1.[1] The awareness of existing or expected fraud will eventually result in the definition of a security policy, with objectives and strategies. The objectives are the basis for a statement (or program) of requirements, which, together with the drafted strategies, will result in the security program (or security scheme).

Both programs are, together with a fraud-risk analysis, the base for the selection of security measures, the security design and the final development of the security product. The various stages of this development sequence will be briefly treated in this article. Attention will further be paid to the iterative aspects of the design process from the standpoint of industrial design.

*VanRenesse Consulting, Willem de Zwijgerlaan 5, 2582 ED The Hague, The Netherlands
Telephone +31 70 3540 333, ruud_van_renesse@zonnet.nl

## 2. SECURITY POLICY

Awareness of a security problem and considering it of sufficient importance are prerequisites for the onset of the development of a product that will solve this problem or at least diminish its undesirable impact. A security policy will then be outlined, comprising objectives and strategies.
***Objectives*** will be formulated explaining what has to be achieved to halt or sufficiently diminish the problem. The experienced or expected problem may be either directly financial or may involve indirect damage to the corporate image because the fraud violates the public trust in the product. The objectives will be further elaborated in the *statement of requirements*. ***Strategies*** will then be drafted that explain how the formulated objectives will be achieved. Detailed solutions will subsequently be the subject of the *security program*.

In table I a few examples are given -naturally not limitative- of subjects that will be relevant to the formulation of objectives and the drafting of strategies.

**Table I - Security policy**

| **Objectives** | **Strategy** |
|---|---|
| product function | product planning |
| target results: commercial | type of fraud |
| technical | required knowledge |
| security | time schedule |
| target dates | co-operation with other parties |
| priorities | budget, investments |
| corporate image | publicity, education |
| ... | personnel |

## 3. FRAUD-RISK ANALYSIS

The fraud-risk analysis involves the following procedure:
1. Define the various methods of attack or fraud.
2. Define/assess the damage involved with each individual method of attack or fraud.
3. Define/assess the probability of occurrence of each individual method of attack or fraud.
4. Calculate/assess each individual risk.
5. Balance each individual risk against the costs of eliminating or reducing it (cost-damage analysis).

This analysis results in a report, which carefully defines and/or assesses the various fraud-risk parameters, involved with the calculation of the (expected) risk. This risk equals the product of the (experienced or expected) damage and the probability of that damage to occur. The various methods of fraud are set out in a table against the damage they cause and their probability of occurrence. In table II a few hypothetical examples are given.

**Table II - Fraud-Risk analysis**

| **Fraud** / **Risk** | theft/ burglary/ robbery | forgery | Counterfeit | | |
|---|---|---|---|---|---|
| | | | origination | copying | imitation |
| Damage | 10 million | 2 million | Large | 400,000 | 50,000 |
| Probability | 0.01 | 1 | very small | 0.5 | large |
| **Risk** | 100,000 | 2 million | acceptable | 200,000 | negligible? |

Each entry in the table has to be discussed and made plausible in the covering report. As it appears, an exact assessment of the

damage, its probability and the subsequent calculation of the risk involved, is neither always possible nor always necessary. A "large" damage, due to an attack like origination, that has been shielded off rigorously, so that its probability is assessed "very small" may be considered "acceptable" as long as this is made plausible in the report. A damage of 50.000 due for example to nuisance counterfeiting may be not worthwhile to pay any attention to and considered "negligible".
Moreover, how will the risk be estimated of damage to the corporate image by fraud obvious to the general public, associated with recurrent publications in the media? The actual damage may be relatively small, but the corporate damage may be unacceptable on the long term. Viewed in that light, the risk of nuisance counterfeiting, after all, may not be "negligible" at all. The risk therefore will be frequently expressed in qualitative terms.

In the first instance the various existing patterns of fraud will have to pass in review. The future however must also be borne in mind: new technologies may lead to completely new methods of fraud. An example is de rapid development of desk-top publishing technology (scanner, computer software, colour printer), by which a considerable desk-top fraud will become possible in the very near future. An extended view into the near future of document fraud is given by the USA National Research Counsil.[2]
Subject of a fraud-risk analysis may also be a discussion of the level of complexity that is involved with various methods of attack, in order to more or less quantitatively demonstrate the expected probability of occurrence.

As figure 1 illustrates, the fraud-risk analysis is embedded in a cost-damage analysis. The assessed risk is balanced against the expected costs involved with curtailing that risk, in order to avoid 'underkill' or 'overkill'. This balance is taken into account by the drafting of the statement of requirements as well as the security program.

The fraud-risk analysis is one of the indispensable documents for the evaluator of the security design/product. It enables him to draw correct conclusions from the security system matrix that he has devised.

## 4. THE STATEMENT OF REQUIREMENTS

The policy, in particular the formulated objectives, as well as the fraud-risk analysis are input to the statement of requirements, which is the starting-point of the product design in a broad sense. Arranging the list of requirements is a complex and critical procedure that methodological rules and checklists have been developed for. Not only physical and chemical requirements have to be met, but also many aesthetic, semantic, ergonomic and security requirements. For example, Optically Variable Devices (OVDs) must resist peeling and wear, have an appealing, conspicuous and unique appearance. OVDs as such offer little security, they must relate to the product and integrate into the product design. Imitation and replication must be made difficult, taking the required level of security in consideration: will the valuable product be a cheap gift voucher, an expensive season travel ticket or an invaluable passport?
First line inspection requires that OVDs are unambiguous, self-explanatory, easily communicated, memorised and recognised. How is this achieved? In section 7 a few considerations will be devoted to ergonomic aspects of OVDs as well as their resistance against counterfeiting. It will appear that requirements may be mutually exclusive in some cases, which results in a trade off between one requirement and the other. In such cases not all requirements can be fully met unless the design is suitably adjusted.

The design of a product will of course be good if it meets the criteria laid down in the statement of requirements. But what criteria must be met by the statement of requirements? In the first place a complete and valid set of requirements must be composed. Checklists and procedures have been published that aid in composing a suitable statement of requirements. Subsequently the program of requirements must be examined, applying six basic criteria.

Table III gives a few examples of items that may appear in checklists and the relevant criteria for the statement of requirements. The statement of requirements must be tested on these criteria: completeness, validity, operability, accessibility, redundancy and length. These criteria will be briefly discussed in the following.

| Table III - Statement of requirements | |
|---|---|
| Checklist: performance<br>environment<br>durability<br>maintenance<br>production costs<br>production facilities<br>material<br>ergonomics<br>quality<br>standards<br>tests<br>security<br>safety<br>... | Criteria: 1. Completeness<br>2. Validity<br>3. Operability<br>4. Accessibility<br>5. Redundancy<br>6. Number of criteria and their importance |

- **Completeness** In order to ensure that the final product indeed meets the expectations, the statement of requirements must be as complete as possible. If essential criteria are overlooked, the final product may not fulfil the functions aimed at. For example, if basic ergonomic requirements are disregarded, an OVD design may become overly complex, and, as a result, inspection may be hindered and the level of first line security significantly decreased. This is where relevant checklists become indispensable.
- **Validity** Criteria must be valid, i.e. they must relate to the desired function. For instance if an OVD aims at raising tamper resistance, the number of yearly tamper cases cannot be a valid criterion, because this number also depends on other factors. Validity is the paramount characteristic that is required of each individual criterion in the statement of requirements.
- **Operability** Criteria must be operable, i.e. it must be possible to establish objectively whether they are met or not. For example, simply requiring an OVD to be appealing or having a harmonious radiance will not do; it must be explained how it will be decided that it indeed meets these criteria. Criteria like reliable, valuable, and convenient, which are frequently mentioned, as requirements are inoperable as such. In some cases a panel of laypersons or experienced experts may settle matters immeasurable. Anyway, the procedure by which the matter will be settled must be already defined in the statement of requirements.
- **Accessibility** Criteria must be accessible, i.e. their verification must be practically possible and the costs and time involved must remain within acceptable limits. Sometimes the problem is the time required to verify if the particular criterion is actually met, in other cases its verification is prohibitively complex and costly. For example the level of complexity of product origination by fraudsters may be very expensive to establish, as this may require the procurement of additional know-how, assembling equipment and performing extensive experiments. On the other hand, experienced external laboratories may perform these tasks, but the time involved or security considerations may be prohibitive. Such predicaments must be foreseen in the statement of requirements.
- **Redundancy** Redundancy of different requirements must be avoided. Certain properties must not count twice or more in the valuation of the product. This situation may ensue if ends and means are not clearly distinguished, so that criteria of a different level end up as autonomous criteria in the statement of requirements. For example criteria for an OVD may be (1) high diffraction efficiency, (2) conspicuousness, (3) being easy to communicate as well as to memorise and recognise and (4) suitability for reliable inspection. These criteria do not belong in one statement of requirements. The first three criteria are means to the end "reliable inspection", while high diffraction efficiency can be considered a means to conspicuousness.
- **Importance** Finally the number of criteria and their weight must be considered. A statement of requirements containing too many product criteria becomes inoperable because a systematic evaluation becomes impossible. Monitoring the relative significance of the criteria helps keeping the length of the statement of requirement within acceptable limits.

The statement of requirements is an indispensable help for the designer to accomplish his task in an efficient and correct manner, without wandering through endless design loops which only slowly, if at all, converge towards the desired product. The effort to create an adequate statement of requirements therefore is not a waste of time. Moreover, without this document a proper evaluation of the design or the final product is unduly laborious. And, last but not least, the formulation of the statement of requirements helps the contractor realise what he actually wants.

## 5. THE SECURITY PROGRAM

The composition of the statement of requirements is in fact already a part of the design process. Different designers may produce different but equally good statements of requirements. The statement of requirements defines the criteria that the design/product has to meet (the solution of the experienced problem); it does not define how that shall be achieved, or anyway should not do this. The statement of requirements is a detailed elaboration of the policy objectives and it is the questionnaire that the contractor presents to the designer.
While the statement of requirements is the detailed elaboration of the policy objectives, the security program is the response to the policy strategies. Moreover, in the security program the policy strategies are elaborated, also taking into account the fraud-risk analysis, the cost-damage analysis and the statement of requirements. The security program describes how the requirements will be met; it is the framework in which all security aspects are treated in their mutual relationships. In the security program objectives and strategies assemble: it is the completed outcome of the outlined policy.

Not only technical, but also organising security measures are dealt with in the security program, which may be considered as a preliminary design on a high conceptual level. Not all procedures and details are specified in detail.

**Table IV - Security program**

| |
|---|
| Technical security measures: |
| - material |
| - commercial availability |
| - production means |
| Organisational measures and procedures: |
| - production |
| - distribution |
| - storage |
| - inspection |
| - education, training: public |
| inspection bodies |
| - transfer of information |
| - document personalisation |
| - catastrophe schemes |
| - upgrading of measures |

Table IV surveys a few possible subjects of the security program. The security program is the base for the pursued security design. On the basis of these data the designer selects the factual operational procedures and the document/product security features. The security design finally is the starting-point for the production of the security product.

## 6. THE DESIGN PROCESS

### 6.1 The function of the product

Starting-point of each design is the desired function of the product to be developed. Not only the technical function, but also possible psychological, economical, social and cultural functions have to be considered. The designer requires at least a rough account of these functions in order to allow him to do a proper job. For example, apart from radiating the corporate image, the

functions of an OVD may comprise the increase of fraud resistance, esthetical attraction as well as market value. As table I indicates, the product function (objective) is already defined as a part of the security policy during the product-planning phase (strategy). The product function is in fact the most important input to the statement of requirements.

### 6.2 The basic design cycle

An existing problem, when experienced as sufficiently annoying, generally results in the definition of the function of a desired product that should partly or wholly eliminate this problem. When the desired function of the product to be developed is defined, an invariable cyclic design process follows: the basic cycle of the design process. This basic cycle is an empirical cycle, a trial and error process, which involves a number of subsequent actions.

**Table V - Parts of the Design Process**

| Action | Result of the action |
|---|---|
| Analysis | List of criteria |
| Synthesis | Design |
| Simulation | Characteristics of the design |
| Evaluation | Value of the design |

As is shown in table V, each of these actions has a certain result. The *analysis* comprises the definition of the problem and the formulation of the objectives. The result is a list of criteria (the base for the final statement of requirements) that the design/product has to meet. Problem as well as function relate to the difference between an undesirable starting point and a desirable ultimate object, a difference that has to be eliminated. The next phase in the basic cycle stands diametrical to the analytic phase. This is the phase of *synthesis* -the creative act- resulting in a preliminary design. Although this synthesis has been characterised as the crucial step in the design cycle, it may not be inferred that other steps are less important or may be omitted. By *simulation* the characteristics of the design are subsequently established, after which an *evaluation* finally leads to an appraisal of the design. This involves assessing in how far the characteristics of the design meet the requirements delineated earlier.

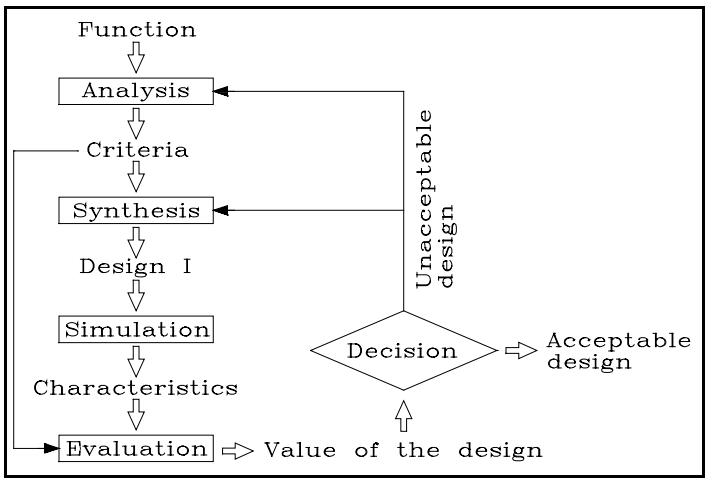


**Figure 2** - The basic design cycle

On the base of this evaluation it can be decided whether the accomplished design is acceptable, or if the basic cycle has to be turned once more. In the latter case the analysis and/or the synthesis have to be executed once more, possibly resulting in an adjustment of the formulated requirements and/or a revised design. The basic design cycle is sketched in figure 2. The actions and their results, listed in table V, are brought together in a cyclic process.

As it appears, security design in general has remained rather an art than having advanced methodologically and scientifically, the way industrial design has in the past decades.
As a further illustration, let us have a brief look at the iterative structure of the design process given in figure 3. This figure, in a somewhat different fashion, illustrates the repetitive character of the basic design cycle. Through each cycle, the design converges further towards an acceptable result. This procedure is typical for each design process, whether a design of a check or that of a complete security system. In fact an effective design process proceeds like this and not otherwise, which makes this design process a normative rule.

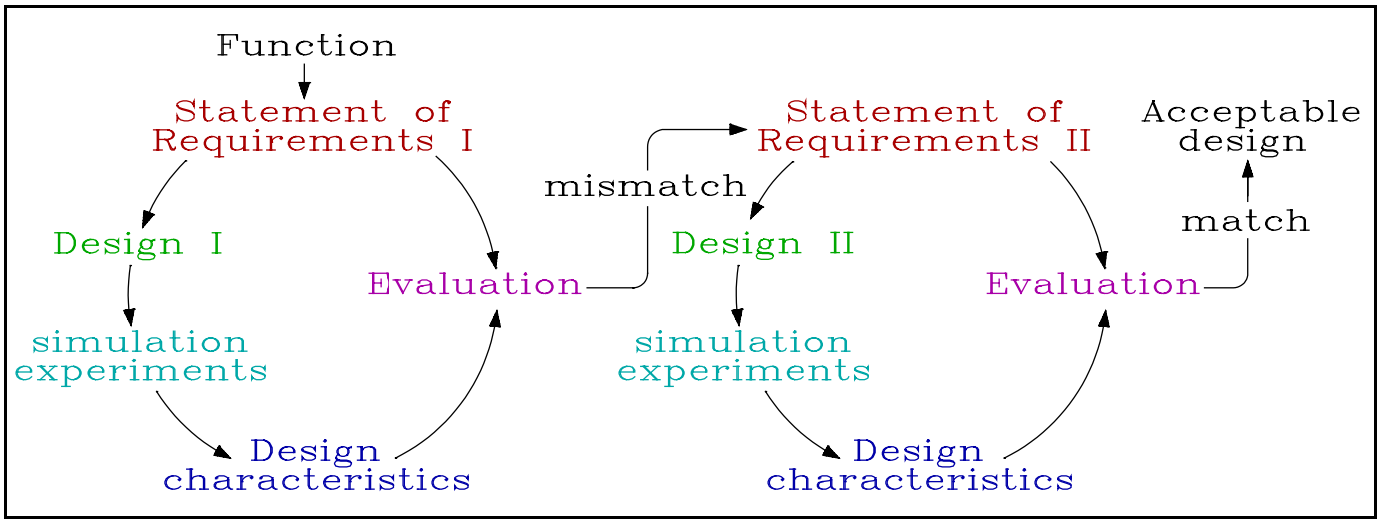


**Figure 3** - The iterative structure of the design process.

### 6.3 The characteristics of the design

From the defined functions the statement of requirements must be derived as a design base. The creative act of designing having taken place, simulation and/or experiments are required to assess the design or product characteristics. In table VI a number of input parameters is specified that plays a role here. Apart from theoretical aspects, this process involves experimental aspects, in particular when it concerns a product or prototype.

**Table VI - Simulation and Experiments**

| | | |
|---|---|---|
| **Input** | theory: | practice: |
| | knowledge<br>reasoning, theories<br>formulas, tables<br>models | research methods<br>model tests<br>laboratory research<br>panel investigations |
| **Output** | (expected) properties of the design/product | |

Experienced knowledge, reasoning, model tests, theories, formulas, tables, etc. may serve this purpose. Once all relevant properties of the design or product are established, they can be compared with the documented criteria. This is the actual evaluation, which further may result in the establishment of weak and strong points and possible paths of attack. In case the evaluation reveals a considerable mismatch between requirements and characteristics, the cycle must be circled again and either the requirements must be adapted, the design, or both. This procedure is repeated until the remaining mismatch between requirements and design properties becomes acceptable. The methodology of evaluation will be treated at this conference as well.[3] Experience teaches that the passing through one single cycle rarely, if at all, results in design or product characteristics that sufficiently match the documented requirements. Convergence towards an acceptable product requires almost invariably the passing through multiple design cycles. Archer has eloquently phrased this course of events:

> *The first thing to recognize is that "the problem" in a design problem, like any other ill-defined problem, is not the statement of requirements. Nor is the "solution" the means ultimately arrived at to meet those requirements. "The problem" is obscurity about the requirements, the practicability of envisageable provisions and/or misfit between the requirements and the provisions. The "solution" is a requirement-provision match that contains an acceptable small amount of residual misfit and obscurity.*[4]

Recognition of this fact is paramount in the stage of security policy definition, when target dates and time schedules are defined. If no adequate room is allowed for the outlined iterative process, invaluable time may be lost with last stage re-designs. Already ordered and delivered material or equipment may appear superfluous or inadequate, a product that does not (fully) match the requirements may have to be settled for, or the target date -which often is an imperative deadline- may have to be exceeded.

The evaluation of subsequent design results is normally performed by the designer. However, it is not always easy for the designer to do this in a completely unbiased manner. There are almost inevitable subconscious tendencies to leap from the experiencing of a problem to the immediate application of countermeasures and to take the required design properties for granted without a proper analysis. This is why it is generally beneficial to have crucial stages of the design examined by an independent evaluator.
As a result of this inclination to shortcut the design cycle, a security policy may not or may be incompletely formulated, a statement of requirements may appear to be either missing or to be critically incomplete from a security point of view and the security program and fraud-risk analysis may be partly or completely missing. The desired properties of the design are taken for granted and are rarely verified methodologically. Evaluations of the design, if any, therefore fail to adequately establish its weak and strong points.

If the finished product, in its final stage, is evaluated by an independent body and its eventual inherent weaknesses are revealed, the damage may be substantial. In this case there may be no love lost between the evaluator and the designer. All the more reason to have an evaluator do his job in an early stage of the process. Subject of an evaluation should not only be the designed product itself, but also the outlined security policy (would the formulated objectives and strategies indeed thwart the threats experienced or expected?), the statement of requirements (does it meet the security policy and the fraud-risk analysis?), the security program (does it realise the requirements and does it answer the security policy as well as the fraud-risk analysis?). Each of these indispensable inputs in the design cycle should be achieved through yet another design cycle. On first sight this may seem a cumbersome procedure, but it is not always realised that methodological tools are offered that help to speed it up and that at the same time this procedure makes the design process more efficient and reliable. In this process the designer and the evaluator, instead of being opponents, become partners in security.

## 7. SOME OVD SECURITY DESIGN CONSIDERATIONS

In section 4 it was stated that inspection of an OVD requires that it is unambiguous, self-explanatory, easily communicated, memorised and recognised. This section discusses a few aspects that pertain to the resistance of OVDs to counterfeiting (remaking) and the consequences this has for first line inspection. This subject is of some importance because organised crime has devoted considerable efforts to counterfeiting OVDs, which efforts have been successful in some cases. This unfortunate development has been generally met by considerably increasing the complexity of OVD images. This approach has severe implications for the ergonomics of security design.

### 7.1 Image complexity

It is generally accepted that counterfeit resistance of diffractive OVDs is an increasing function of their image complexity. In fact several hologram-manufacturing companies explicitly propagate the high image complexity of their products as an advantageous property that thwarts counterfeiting. In other cases the number of proposed optical and graphic effects and their combinations appears next to bewildering. And indeed, in practice, security OVDs are produced that are so complicated that the unambiguous communication of their image properties as well as their recollection becomes virtually impossible. To the opinion of this author, this must be considered a major violation of sound security design rules.

The OVD design should be 'self-explanatory'; i.e. it must become evident for the acceptor what too look for, if need be even without a preceding verbal communication.[5] This 'self-explaining' property will allow the description of relevant effects that the acceptor has to look for, in but a few simple words. This description must uniquely and unambiguously relate to the specific effect, while the briefness of the description must not result in vagueness.

As a consequence, the following subset of (partly redundant) requirements holds:

- The OVD image contents must be obvious and identifiable (recognisable).
- The OVD image must unambiguously relate to the product it protects.
- The OVD image must convey a message relevant to the product and its function.
- The image elements must be easy to communicate. Consequently, there must not be too many image elements and/or optical effects.
- The image contents must be easy to memorise. Consequently the image may not be very complex.
- The optical effects must be interdependent (coherent or self-referencing), this coherence must be obvious and should be easily communicated.
- The image contents must not have existing competitors, which may serve as successful imitations.

Contrary, the pursued complexity of image content of OVDs is regarded as equivalent to advancement and sophistication by their originators. This image- or visual complexity is associated with the number of reconstructed first order channels, the number and intricacy of image elements and the number and intricacy of possible kinematic- and colour effects. It may be noted that such OVD parameters are completely brought about by diffraction elements, characterised by practically uniform azimuth and pitch and diffraction grooves with practically sinusoidal section profiles. Alternatives to these properties will be discussed in the next section.

Figure 4 schematically illustrates the relation between counterfeit resistance and image complexity. On the low end we find simple images that, consequently, can be easily counterfeited. Such images tend to be self explanatory, and easily communicated, remembered and recognised. Therefore, their first line inspection is easy, but, understandably, our confidence in their authenticity remains relatively low.

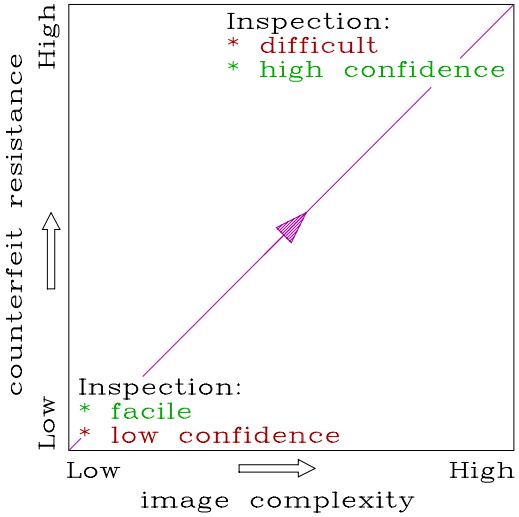


**Figure 4** - Counterfeit resistance is an increasing function of image complexity. (No complex structures involved).

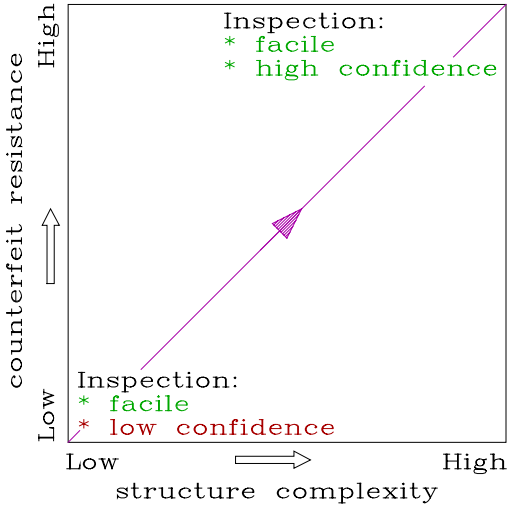


**Figure 5** - Counterfeit resistance is an increasing function of structure complexity. (No complex images involved).

This observation leads to a brief but necessary discussion of existing opinions on the practical use of OVDs for security. Widely conversed events are those of inspectors that react in surprise on the deliberate replacement of a genuine and simple OVD (e.g. of a dove) by a fake one (e.g. of a rabbit) with words like "*Oh look, they changed the hologram!*". Frequently, this typical reaction is unmindfully presented as proof of the ultimate uselessness of OVDs. This is most unfortunate, because such an occurrence actually proves that the recognition of the deviation was immediate, once it was looked for. The naive conclusion, drawn by the inspector, that the original OVD was legitimately substituted by another, does not prove anything about the potential of OVDs. It only proves that training and information of the inspector was lacking.

And again, the frequently expressed, nonchalant and rejective pronouncement that "*if it's shiny, they'll accept it*" does not prove the uselessness of OVDs, but rather proves the impossibility of adequate inspection due to design complexity, the lack of adequate public information, or both. Such information and training may become more efficacious if the above rules for security design are taken into account.

And this not only counts for the security design, but also for the provided information, which sometimes completely lacks comprehensibility and legibility! Contrary, the introduction of complex images will most certainly impede the adequate training of the public as well as professional inspectors like bank tellers.

On the high end of the graph in figure 4 we find very complex images that are expectedly difficult to counterfeit. Although we may have a high confidence in their authenticity, such complex images are not likely self-explanatory and they tend to be difficult to communicate, remember and recognise. Therefore, their first line inspection is considerably more demanding.
In general we may expect a tendency to omit an adequate first line inspection of complex OVDs and indeed a tendency of taking them for granted as long as they are shiny! Obviously, in this case, a trade off exists between the ease of inspection in first line and the confidence that we have in authenticity of the security feature. The conclusion is, that overly increasing the complexity of OVDs, in order to considerably raise their counterfeit resistance, leads to dangerously overshooting the mark.

### 7.2 Structure complexity

A supplementary thesis is, that counterfeit resistance is an increasing function of structure complexity. This second thesis is schematically illustrated by figure 5. This subject has been addressed extensively in an earlier paper.[6] Structure complexity is associated with the amount of order that is contained in the OVD, on a microscopic, sub-micron, or even on a molecular scale. This fine structural order may be brought about by non-uniformities in diffraction structures, asymmetric cross-sections of diffraction grooves, sub-wavelength 3D detail of diffraction grooves, interference structures, and order on a molecular level. Table VII presents an overview.

**Table VII** - overview of complex security structures based on diffraction and interference

| device type | structure characteristics | examples |
|---|---|---|
| Pixelgram, exelgram | Non-uniform distribution of azimuth and pitch of diffraction grooves | Australian "Opal stamp", Vietnam Bank Check |
| Kinegram | Asymmetric cross-sections of diffraction grooves | Netherlands Postcheque "Einstein", Swiss ID-card |
| Zero order devices (ZODs) | Sub-micron three-dimensional high refractive index diffraction structures embedded in low index matrix | Diffractive Identification Device (DID), commercial applications currently being developed |
| Thin film interference coatings | Multilayer composite interference structures | Canadian bank notes, Optically Variable Ink (OVI) on various bank notes |
| Polymerised liquid crystals | Helical molecular organization of interference layers in cholesteric liquid crystal phase | Advantage seal and Identiseal on various valuable documents |

Techniques to achieve structure complexity are interferometry and holography combined with chemical differential etching and ion beam etching, electron beam lithography, electron beam modulation techniques, thin film vacuum technology, liquid crystal- and liquid crystal polymer technology.
On rotation of the security feature, such structural order may result in positive-negative image swaps (pixelgram), reverse in contrast between first diffraction orders (kinegram), and well defined colour conversions (DID, thin film composites, OVI and liquid crystals). These optical effects are unusual, conspicuous and well defined, and therefore tend to sustain easy communication, recollection and recognition, which in their turn allow efficient inspection in first line. At the same time these optical effects are very hard to counterfeit, so that their first line inspection may provide a high confidence in authenticity as well. The image content may remain very simple while the optical effects are based on complex structures. Obviously in this case a combination is achieved of easy inspection in first line and a high confidence in authenticity of the security feature.

### 7.3 Nano-technology versus ergonomics

Considering both cases, that of image- and structure complexity, and their apparent consequences for security design, a gradual shift from complex OVD images towards simple OVD images with complex structures, can be foreseen. This is only a logical continuation of the ongoing progress of nano-technology, which has lifted security features to their current advanced state. Mankind has learned to sculpture matter with nanometer precision, so that matter has become a virtually unlimited recording medium that is only beginning to reveal its seemingly magic potential. One of the results of this technological development is, that matter can be shaped into extremely precise diffractive and interference elements, rendering unexpected and highly uncommon optical effects that are extremely difficult to counterfeit, can be easily verified and yet can be economically mass produced. Moreover, intricate machine readable codes can be incorporated in security devices, thus rendering them additional and powerful second line security potential (with the use of tools, like a magnifier, an ultraviolet source, an inspection machine, etc). It would seem that, on the long run, these remarkable advancements of nano-technology will enable us to largely eliminate document fraud and product piracy.
There is a "but" though, associated with this seemingly bright view on the future. Nano-technology security features, however powerful, are useless if they are not adequately inspected. And adequate inspection in first line becomes only possible if security design follows at least some basic ergonomic rules. Here we enter a field that has scarcely been set foot on until now, and this field seems to be as bare as the field of nano-technology is profuse. It appears paramount therefore that fundamental and practical research on ergonomic security design is carried out in the near future.

## 8. DISCUSSION

Although the examples given in this paper mostly relate to optically variable devices (OVDs), this does not imply that the discussion on security design is limited to OVDs. The systematic approach of security design discussed is generally valid for security design of documents, products and systems. The fact that security design is not very frequently approached methodologically may be caused by the subconscious inclination to solution directed thinking. This involves the immediate brainstorming for solutions after the experience of a problem and the selection of the seemingly best solution. This approach is based on the idea that it is the fastest way to success. As a result solutions are frequently pursued that finally appear to be sub-optimal, inadequate or not realistic. Valuable time is lost by this approach, which might otherwise have been devoted to the approach of problem directed thinking. In the latter approach, the problem and the relevant functions of the product that must solve the problem are defined as exactly as possible, and subsequently the four basic design actions analysis, synthesis, simulation and evaluation are performed (see section 6). The seemingly time consuming aspects of this approach tend to have a discouraging effect; but it must be borne in mind that the alternative of jumping to solutions may actually consume at least as much time, while possibly not rendering the desired result.

## 9. REFERENCES


1. R. Tadema Wielandt, "The evaluation of document fraud resistance", *Optical Document Security*, R.L. van Renesse (ed), chapter 2, Artech House, Boston/London 1993.
2. National Materials Advisory Board, Commission on Engineering and Technical Systems, National Research Council, *Counterfeit Deterrent Features for the Next-Generation Currency Design*, Publication NMAB-472, National Academy Press (1993).
3. J. Pieters, "Trends in security evaluation", SPIE Conference on Optical Security and Counterfeit Deterrence Techniques, San José, Ca., January 28 - February 2, 1969, SPIE vol. 2659-03.
4. L.B. Archer, "Whatever became of design methodology?", *Design Studies*, 1 (1979) 1, p. 17-18.
5. J.-F Moser, "Document protection by Optically Variable Graphics (Kinegram)", *Optical Document Security*, R.L. van Renesse (ed), chapter 9, Artech House, Boston/London 1993.
6. R.L. van Renesse, "Ordering the order - a survey of optical document security features", *SPIE vol. 2406, Conference on Practical Holography IX*, San José, Ca., 5-10 February 1995, p. 268 - 275.