A Logo Gestalt based Framework for Brand Services

Pablo A. Valle
Technical University Berlin
Faculty Mechanical Engineering and Transportation Systems
Strasse des 17. Juni 135, 10623 Berlin, Germany
valepnbb@mailbox.tu-berlin.de

Raul Vicente Garcia
Fraunhofer IPK
Dept. Security Technologies
Pascalstr. 8-9, 10587 Berlin, Germany
raul@ipk.fraunhofer.de

Mario Köppen
Kyushu Institute of Technology
Dept. Artificial Intelligence
680-4, Kawazu, Iizuka, Fukuoka 820-8502 Japan
mkoeppen@pluto.ai.kyutech.ac.jp

Abstract

In this paper, we are considering the web-based services related to product brands, so-called Brand Services, more closely, and propose a framework for the provision of such services. The framework is suited to the particular needs of such services, in particular for supporting brand protection against forgeries, as well as the sustainability of market competition by covering product quantity and quality related information. Main idea is the separation between an application service, and a brand service guarding service. With the addition of storing information in a logo or scheme by Gestalt based information hiding, entailment and control over the distributed information can be achieved. For the user, the framework appears seemless, as he just delivers a product identifier found on the purchased product, and receives corresponding information.

1. Introduction

By current estimates of EU commision, product forgery is causing an economical loss of 300 Billion Euro per year. A number of 7 to 9% of products on the market are considered to be forgeries. The tendency is increasing. Together with the economical damages, also cultural damages as well as loss of working places and threats to health and safety of customers have to be taken into account. The most common measure for product quality and functionality is its brand. The brand of a product is a direct reference to its producer, and ensures better design, and product related services. But the extra effort related to this manner of product maintenance is also causing higher costs, and a lower position in a market competing for low costs. However, proof of authenticity of a product is still the main interest of the customer.

Means for such proofs are sparse. Often, the customer is left to himself by verifying information with vendor information distributed via the internet, or by seeking external advice. Here, we are considering web based services for establishing the link between the producer and its customer. For ensuring several demands on such a framework, we introduce the concept of brand services. A framework for such services will be introduced in section 2. Then, section 3 gives means for adding security to the distributed information, which is based on Gestalt laws to identify components of a visual cue (logo, product scheme) that can be used for information storage. The paper concludes with a short summary.

2. Brand Services

By the term Brand Services, we understand all services that are primarily related to the brand character of a good. Among such services we can find

- release of information about the product or product series
- release of information about the producer
- proof of authenticity of a product for detecting forgeries

Proceedings of the International Conference on
Next Generation Web Services Practices (NWeSP'06)
0-7695-2664-0/06 $20.00 © 2006 IEEE

- measures for increasing product awareness
- supporting the mapping of brands to products
- on-line retrieval of brand products

To establish such services, a distributed application framework with a central data maintenance will be proposed. The framework has to fulfill specific demands on data security and data integrity, related to the centralised aspects of e.g. information storage about products and brands of potentially competing producers. Therefore, there is a need for anonymisation of stored information. Otherwise, unauthorized access or unintended spread of sensitive information might influence market position of a producer that participates in the brand service provision.

Such a goal can be achieved by the establishment of a cryptographic infrastructure:

- central data storage in trust centers
- public-private key infrastructure, esp. the use of digital signatures
- zero-knowledge protocols for anonymisation

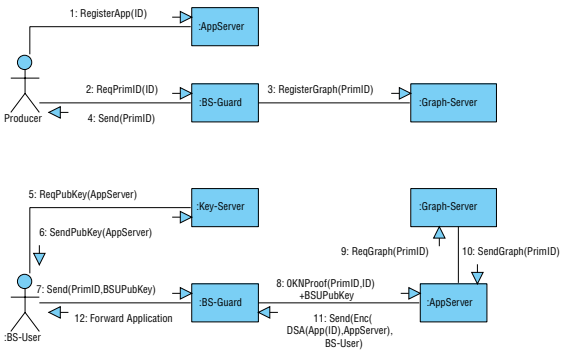

Figure 1. Brand service framework.

Consider the following use case of such a framework: a producer wants to tag one of its products with a 2d-barcode that contains the information about a website. The website provides more detailed product information. Besides the obvious notion of providing information related to advertisement, this information could be also about selected features of the product that help to ensure authenticity of the product.

The simplest approach would be to store the url of the website directly into the barcode. However, such an approach has major disadvantages that count much in the context of brand protection: the following access to the website can neither be entailed (e.g. it cannot be modified after printing and distribution of the barcode), nor controlled by the producer. In parallel to supporting the customer, its also supporting the potential brand forger.

Figure 1 shows the proposed framework. Countermeasures for the named two disadvantages, lack of entailment and lack of control can be found in the following two paradigms:

- introduction of a product information reference instead of direct information by means of an *Application Server* (:AppServer), and
- introduction of a buffering instance between the user of a brand service and the reference access, by means of a *Brand Service Guard* (:BS-Guard).

The framework then is used in the following manner:

1. Two identifiers (e.g. dataset ids in a database) are used for the management of product information. Before releasing the tagged product series, the producer registers and stores product information (or an application program or program extension) on :AppServer and receives an identifier ID. This identifier uniquely references the stored information or product related application. This could be information about a larger number of security features of the product, or a mobile application that can be issued to the customer later on, for doing integrity check by herself. Upon delivery of a particular product, the producer demands a second identifier, the $PrimID$, from the :BS-Guard. The identifier ID is needed for obtaining such a $PrimID$. The $PrimID$ is randomly generated by the :BS-Guard from ID and delivered to the producer. Now, the producer can store the $PrimID$ on the product directly, as will be detailed below. At the same time, the Brand Service Guard registers the relation between ID and $PrimID$ by using a zero knowledge algorithm. Brand Service Guard's "knowledge" about the relation between these two identifiers is used to modify a one-way function correspondingly. A simple illustration for this can be done by using Hamiltonian graphs that are permuted according to numerical values derived from the identifiers, and randomly filled with further vertices to hide the Hamiltonian path in the graph [1]. The graph is stored on an external server, the *Graph Server* (:Graph-Server) together with the $PrimID$ for reference. Later on, by this means the :BS-Guard can proof its knowledge about the relation between ID and $PrimID$ without revealing this relation to a 3rd party(so-called Zero-Knowledge Proof).

2. The producer then stores $PrimID$ on the product, by e.g. printing it into a barcode, RFID, or by using a digital watermarking technique, and delivers the product.

3. Once a customer wants to use the brand service related to the product that he purchased, he scans the $PrimID$ from the product (e.g. by using a mobile application) and sends it to :BS-Guard. The customer (or the application that he using for scanning) also accesses the public key of the application server. Thus, also the customer can ensure the validity of the information (or application) that he is going to receive. Finally, the customer sends $PrimID$, and his public key to :BS-Guard.

4. Only :BS-Guard may access the application server, and never the customer directly. For :BS-Guard to access the application server, it needs to proof that it was the one establishing the relation between an ID (the reference for the product series) and a $PrimID$ (found on the product). The proof is done by a zero-knowledge protocol issued by the application server and also using the stored information on the :Graph-Server. If the proof is successful, the :AppServer encodes the information or application referenced by ID with the public key of the customer, digitally signs it by using its own private key, and returns via the :BS-Guard to the customer. The customer checks the signature, and decodes the information or application.

The separation between Application Server and Brand Service Guard ensures the distribution of the relevant information. The Brand Service Guard only knows about mappings of identifiers. It does not learn about the reason to request the $PrimID$. Its also possible for the producer to request additional camouflage identifiers. Thus, information like quantity of produced goods can be covert, and competing producers may coexist within this service. On the other hand, the Application Server only distributes information or application, without learning about the usage or distribution parameters. Nevertheless, both services have to be realized as trust centers, to ensure the separation.

For the user of the brand service, the service itself is seamless: he just sends an identifier found on the product to an entity, and receives the information or information serving and handling application.

3. Gestalt Laws for Information Delivery

The foregoing section gave the means for the distribution of information about a product. For further

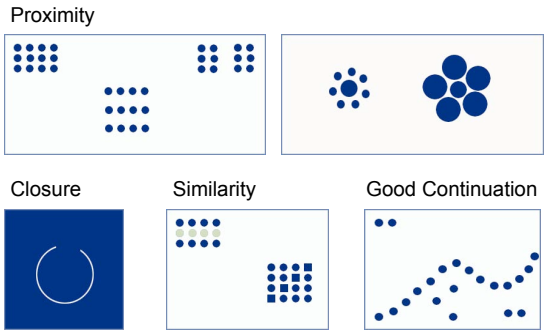

Figure 2. Typical Gestalt laws.

securing the information, a watermarking technology based on Gestalt theory is studied. Here, we are considering information that is given by visual cues, including e.g. the company logo image, or schematic images of the product. Usually, the design of a logo or scheme is supposed to be remarkable, and easy to recognize and to remember.

Figure 3. Modification of a logo: left figure is the original logo, following two grouping Gestalt laws. Next right is a modified version where the Gestalt law of the circles forming a circle itself has been affected, and the modification is easily perceivable. Such modifications should be avoided. The right-most image then shows a modification of the same strength (2px shift) but applied to the inner text block, thus not affecting any Gestalt law. This modification is hardly perceivable, and can be used for information storage.

However, such media content can be copied and used in an unauthorized manner, e.g. for selling forged products via the internet. As the copying cannot be prevented itself, new security technologies like digital watermarking can help to monitor the distribution of media, to prove the origin of media data, or to validate the integrity of data. While often seen as a tricky document processing method, only known to a limited number of people, watermarking is also a kind of information storage, with the main features:

- reusability of space already representing other data of a document
- retrieval based on computer evaluation
- write once, read often paradigm
- lower storage capacity

Among the possible modifications establishing a digital watermark, the modification of logos and schemes is an option that has not been considered much in the past. The simple nature seems to hinder modifications related to information hiding. The question then comes up, which components of a logo can be modified without disturbing the visual impression of a logo or scheme.

Here, we are considering the relevance of Gestalt laws for the design of logos. Gestalt theory is considering grouping based on one or more common characteristics of points or visual objects as the main process in our visual perception [3][2]. In addition, this grouping principle is recursive and allows for the perception of groups of groups according to common characteristics as well. Gestalt is considered the entailment of cognition in the primary perception, in addition to the sensor stimulation from the outer world.

Main thesis is that the Gestalt laws also apply to the design of brand logos and product schemes. Logos and schemes can be remarkably modified, as long as their inherent Gestalt laws are not violated. On the contrary, violations of Gestalt laws can become immediately perceivable. For example, consider a logo text, where in a row of letters the letters are randomly shifted up and down. The change is remarkable, even if the letters are shifted by a few pixel only. In contrary, the complete row of letters as a "Gestalt group" can be moved or scaled heavily, without the change becoming noticable. This also means that impercible modifications of logos can be achieved by modifying logos in a manner that the Gestalt laws governing the logo or scheme design are preserved. See fig. 3 for an example.

The means for modifying logos or schemes are particularly related to the following Gestalt laws (see fig. 2):

- Proximity: We tend to group nearby objects.
- Closure: We are so accustomed to seeing closure that we sometimes close things that aren't.
- Similarity: We tend to group objects with similar properties (color, shape, texture).
- Good continuation: We tend to assign objects to an entity that is defined by smooth lines or curves.

The procedure for the logo or scheme Gestalt then is prepared as follows:

1. Identification of the components of the logo that follow Gestalt laws.
2. Specification of the allowed transformations of the component with respect to the corresponding Gestalt law.
3. Specification of an encoding scheme.

The framework then is implemented by the following three subsystems:

The Gestalt identification subsystem:

1. The logo image is segmented, to yield logo components.
2. To each component, component features are assigned: main color, texture, shape.
3. To each component, spatial features are assigned: nearest other components, position and kind of keypoints of the component.
4. Subsets are selected with similar features, elements being close horizontal or vertical continuation.
5. Gestalt laws are verified by probability of occurrence.

The Gestalt-preserving transformation subsystem:

1. Rules are selected that conclude on a set of allowed transformation, where the condition is the specific fulfillment of a Gestalt law in the logo components.
2. The set of allowed transformations for the logo is identified.
3. A valid subset is randomly selected and put into numerical degree parameters.
4. The degrees are mapped to a permutation sequence of n values.

The Gestalt-encoding subsystem:

1. A number p out of $n!$ is taken that specifies the information that should be stored in the logo.
2. The corresponding permutation gives the ranking of the transformations, means the first one is to be applied strongest, the last one weakest.
3. The transformations are applied, and the now-encoding logo image or scheme is delivered.

The reading of the information is based on a stored reference to the used encoding scheme, and can be integrated into the application that is delivered to the user of a brand service.

4. Conclusion

We have presented a distributed framework for the implementation of brand services. The framework demonstrates the possibility of providing web services related to brands that fulfill contradicting demands: the customers need for simplicity and transparency, the producers needs for publishing and protecting brand information at the same time, the interest of the producer to stay competetive within the market, and the interest of the brand service provider to provide attractive and reliable services. The framework is based on the combination of state of the art cryptographics methods, especially zero knowledge proofs, trust centers and public-private key infrastructure, and information storage in images by means of preserving Gestalt laws that are fulfilled by the logo or scheme design.

Acknowledgment

Authors would express their thanks to unknown referees of this paper for their helpful comments. Authors also wish to thank JSPS fellowship program and CONACYT Mexico for supporting this work.

References

[1] S. Craver. Zero knowledge watermarking. In F. Petitcolas, editor, *Information Hiding - 5th Intl. Workshop*. Springer LNCS, 2002.

[2] G. Kanisza. *Grammatica del Veder*. Il Mulino, Bologna, 1980.

[3] M. Wertheimer. Untersuchungen zur Lehre der Gestalt. *Psychologische Forschung*, 4:301–350, 1923.