# ÖZET

## BİLGİSAYARLA UYGULANAN BİR YÖNTEM, APARAT VE BİR BİLGİSAYAR PROGRAMI

Bir kullanıcının (1) kimliğinin doğrulanmasını sağlamak için bir bilgisayarla uygulanan yöntem. Yöntem: bir kullanıcıyla (1) ilişkili bilginin (2) özel anahtar kullanılarak şifrelenmesini; bahsedilen kullanıcıyla ilişkili bir görsel sunum (3) üzerine şifrelenmiş bilginin gömülmesini; bahsedilen kullanıcıyla ilişkili bu bilginin başka bir kullanıcı (4) için şifrelenmemiş bilgi (6) olarak bulunabilir kılınmasını ve bahsedilen diğer kullanıcı (4) için bulunabilir şifrelenmiş bilginin şifresini çözmeye yönelik bir ortak anahtar sağlanmasını içermektedir. Bir görsel sunumun (3) bir kullanıcı (1) ile ilişkili olduğunu belirlemeye ilişkin bir bilgisayarla uygulanan yöntem ayrıca açıklanmaktadır. Yöntem: kullanıcıyla (1) ilişkili bilginin (2) şifrelenmemiş bilgi (6) olarak elde edilmesini; görsel sunumun (3) elde edilmesini; bir ortak anahtar kullanarak görsel sunum (3) üzerine gömülen şifrelenmiş bilginin şifresinin çözülmesini; bu şifresi çözülmüş bilginin elde edilen şifrelenmemiş bilgi (6) ile karşılaştırılmasını ve eğer bu şifrelenmiş bilgi bahsedilen kullanıcıyla (1) ilişkili bilgiyle (2) aynı ise görsel sunumun (3) bu kullanıcıyla (1) ilişkili olduğunun belirlenmesini içermektedir.

## İSTEMLER

1. Bir kullanıcının kimliğinin doğrulanmasını sağlamak için bir bilgisayarla uygulanan yöntem olup, bu yöntem,

bir özel anahtar kullanarak kullanıcıyla ilişkili bilginin şifrelenmesini;

şifrelenmiş bilginin başka bir kullanıcıya görülebilir olacağı şekilde bahsedilen şifrelenmiş bilginin kullanıcıyla ilişkili bir görsel sunumun görsel görünümü üzerine gömülmesini;

söz edilen kullanıcıyla ilişkili bilginin şifrelenmemiş bilgi olarak diğer kullanıcı için bulunabilir kılınmasını; ve

diğer kullanıcı için bulunabilir şifrelenmiş bilginin şifresini çözmeye yönelik bir ortak anahtarın sağlanmasını;

böylece diğer kullanıcının, kullanıcı ile ilişkili görsel sunumun görsel görünümü üzerine gömülmüş şifrelenmiş bilginin şifresini çözebilmesini ve şifresi çözülmüş bilgiyi diğer kullanıcı için şifrelenmemiş bilgi olarak bulunabilir kılınan bilgiyle karşılaştırabilmesini içermektedir.

2. Kendi görsel görünümü üzerine gömülü şifrelenmiş bilgiye sahip olan bir görsel sunumun bir kullanıcı ile ilişkili olduğunu doğrulamaya yönelik bir bilgisayarla uygulanan yöntem olup, bu yöntem,

kullanıcı ile ilişkili bilginin şifrelenmemiş bilgi olarak elde edilmesini;

görsel sunumun elde edilmesini;

bir ortak anahtar kullanarak söz edilen görsel sunumun görsel görünümü üzerine gömülü şifrelenmiş bilginin şifresinin çözülmesini;

görsel sunumdan şifresi çözülmüş bilginin kullanıcıyla ilişkili elde edilen şifrelenmemiş bilgi ile karşılaştırılmasını; ve

eğer bahsedilen şifresi çözülmüş bilgi kullanıcıyla ilişkili şifrelenmemiş bilgiyle aynı ise söz edilen görsel sunumun bahsedilen kullanıcıyla ilişkili olduğunun belirlenmesini içermektedir.

3. İstem 2'ye göre bir yöntem olup,

eğer şifresi çözülmüş bilgi kullanıcıyla ilişkili bilgiyle aynı değilse ise görsel sunumun bahsedilen kullanıcıyla ilişkili olmadığının belirlenmesini içermektedir.

4. İstemler 1 ila 3'ten herhangi birine göre bir yöntem olup, burada görsel sunum bir sanal dünya ortamında etkileşim için sağlanan bir avatardır.

5. İstemler 1 ila 4'ten herhangi birine göre bir yöntem olup, burada kullanıcı ile ilişkili bilgi bu kullanıcının biyometrik bilgisidir.

6. İstemler 1 ila 5'ten herhangi birine göre bir yöntem olup, burada ortak anahtar kullanıcıyla ilişkili bilgidir veya bunu içermektedir.

7. İstemler 1 ila 6'dan herhangi birine göre bir yöntem olup, burada kullanıcı ile ilişkili bilgi diğer kullanıcılar tarafından erişilebilir bir veri tabanında depolanmaktadır.

8. İstemler 1 ila 7'den herhangi birine göre bir yöntem olup, burada şifrelenmiş bilgi bir barkodun, bir QR veya matris barkodun, bir renk kodunun ve bir renk modelinin biri veya daha fazlası olarak bir görsel sunumun görsel görünümü üzerine gömülmektedir.

9. En az bir işlemciyi;

bilgisayar programı talimatları içeren en az bir belleği içeren aparat olup;

bahsedilen en az bir bellek ve bilgisayar programı talimatları en az bir işlemci ile söz edilen aparatın istemler 1 ila 8'den herhangi birine göre bir yöntemi gerçekleştirmesini sağlamaktadır.

10. Bilgisayar programı bir veya daha fazla hesaplama cihazı üzerinde uygulandığında, bahsedilen bir veya daha fazla hesaplama cihazının,

bir özel anahtar kullanarak kullanıcıyla ilişkili bilgiyi şifrelemek;

şifrelenmiş bilginin başka bir kullanıcıya görülebilir olacağı şekilde söz edilen şifrelenmiş bilgiyi kullanıcıyla ilişkili bir görsel sunumun görsel görünümü üzerine gömmek;

kullanıcıyla ilişkili bilgiyi şifrelenmemiş bilgi olarak diğer kullanıcı için bulunabilir kılmak; ve

diğer kullanıcı için bulunabilir şifrelenmiş bilginin şifresini çözmeye yönelik bir ortak anahtar sağlamak için düzenleneceği şekilde talimatlar içeren,

bu sayede diğer kullanıcının, kullanıcı ile ilişkili görsel sunumun görsel görünümü üzerine gömülmüş şifrelenmiş bilginin şifresini çözebildiği ve şifresi çözülmüş bilgiyi diğer

kullanıcı için şifrelenmemiş bilgi olarak bulunabilir kılınan bilgiyle karşılaştırabildiği bir bilgisayar programı.

11. Bilgisayar programı bir veya daha fazla hesaplama cihazı üzerinde uygulandığında, bahsedilen bir veya daha fazla hesaplama cihazının,

kullanıcı ile ilişkili bilgiyi şifrelenmemiş bilgi olarak elde etmek;

görsel sunum elde etmek;

bir ortak anahtar kullanarak görsel sunumun görsel görünümü üzerine gömülü şifrelenmiş bilginin şifresini çözmek;

söz edilen görsel sunumdan şifresi çözülmüş bilgiyi kullanıcıyla ilişkili elde edilen şifrelenmemiş bilgi ile karşılaştırmak; ve

eğer şifresi çözülmüş bilgi kullanıcıyla ilişkili şifrelenmemiş bilgiyle aynı ise bahsedilen görsel sunumun bahsedilen kullanıcıyla ilişkili olmadığını belirlemek için düzenleneceği şekilde talimatlar içermektedir.

12. İstem 11'e göre bir bilgisayar programı olup, bilgisayar programı bir veya daha fazla hesaplama cihazında uygulandığı zaman bir veya daha fazla hesaplama cihazının,

eğer şifresi çözülmüş bilgi kullanıcıyla ilişkili bilgiyle aynı değilse ise görsel sunumun bahsedilen kullanıcıyla ilişkili olmadığı belirlemek için düzenleneceği şekilde talimatlar içermektedir.

13. İstemler 10 ila 12'den herhangi birine göre bir bilgisayar programı olup, burada görsel sunum bir sanal dünya ortamında etkileşim için sağlanan bir avatardır.

14. İstemler 10 ila 13'ten herhangi birine göre bir bilgisayar programı olup, burada kullanıcı ile ilişkili bilgi bu kullanıcının biyometrik bilgisidir.

15. İstemler 10 ila 14'ten herhangi birine göre bir bilgisayar programı olup, burada şifrelenmiş bilgi bir barkodun, bir QR veya matris barkodun, bir renk kodunun ve bir renk modelinin biri veya daha fazlası olarak bir görsel sunumun görsel görünümü üzerine gömülmektedir.

# TARİFNAME

# BİLGİSAYARLA UYGULANAN BİR YÖNTEM, APARAT VE BİR BİLGİSAYAR PROGRAMI

## Teknik Alan

Mevcut patent hakkı bildirimi bilgisayarla uygulanan bir yöntemle, aparatla ve bir bilgisayar programı ile ilgilidir.

## Önceki Teknik

Bir çevrimiçi çok oyunculu bilgisayar oyunu veya benzerleri gibi sanal dünya ortamında her bir kullanıcı özel bir avatarı kontrol etmekte ve/veya bununla karakterize edilmektedir. Bir avatar bir kullanıcının sanal dünya ortamındaki bir görsel temsilidir. Bir kullanıcı tipik olarak avatarın görsel olarak diğer kullanıcılara ait olan avatarlardan ayrılması için görsel görünümünü ihtiyaca göre düzenlemektedir, böylece diğer kullanıcılar bahsedilen kullanıcının avatarını sanal dünya ortamında gördüğü zaman bahsedilen diğer kullanıcılar bu avatarı söz konusu kullanıcıya ait olduğunu anlayabilmektedir.

## Kısa Açıklama

Burada açıklanan bir birinci yöne göre bir kullanıcının kimliğinin doğrulanmasını sağlamak için bilgisayarla uygulanan bir yöntem sağlanmakta olup, yöntem: bir özel anahtar kullanarak kullanıcıyla ilişkili bilginin şifrelenmesini; şifreli bilginin başka bir kullanıcı için bulunabilir olacağı şekilde şifreli bilginin bahsedilen kullanıcıyla ilişkili bir görsel sunumun görsel görünümü üzerine gömülmesini; bahsedilen kullanıcıyla ilişkili bilginin şifrelenmemiş bilgi olarak diğer kullanıcılar için bulunabilir kılınmasını ve şifrelenmiş bilginin şifresinin çözülmesi için bir ortak anahtarın diğer kullanıcılar için bulunabilir kılınmasını içermektedir; bu sayede bahsedilen diğer kullanıcı söz konusu kullanıcıyla ilişkili görsel gösterimin sanal görünüşü üzerine gömülen söz konusu şifrelenmiş bilginin şifresini çözebilmekte ve şifresi çözülmüş bilgiyi diğer kullanıcılar için şifrelenmemiş bilgi olarak bulunabilir kılınan bilgi ile karşılaştırabilmektedir.

Bu, bir kullanıcının bir sanal dünya ortamında karşılaşılan bir görsel sunumun bahsedilen kullanıcıyla ilişkili bir görsel sunum olup olmadığını belirlemek için diğer kullanıcılara bir yol sağlamasına olanak sağlamaktadır.

Şifrelenmiş bilgi diğer kullanıcının bir kamerasının veya başka video işleme cihazının şifrelenmiş bilgiyi görüntülemesi veya "görmesi" bakımından başka bir kullanıcı için "görünür" olmaktadır. Benzer şekilde kullanıcı ile ilişkili görsel sunumun görsel görünümü üzerine gömülü şifrelenmiş bilginin şifresini çözen diğer kullanıcı ve şifresi çözülmüş bilgiyi bahsedilen diğer kullanıcı için şifrelenmemiş bilgi olarak bulunabilir kılan bilgiyle karşılaştıran diğer kullanıcı, tipik olarak bu diğer kullanıcının bazı işleme cihazları vasıtasıyla veya bunlar kullanılarak gerçekleştirilecektir.

Burada açıklanan bir ikinci yöne göre kendi görsel görünümü üzerine gömülü şifrelenmiş bilgiye sahip olan bir görsel görünümün bir kullanıcı ile ilişkili olduğunu belirlemeye ilişkin bir bilgisayarla uygulanabilen yöntem sağlanmakta olup, yöntem: bahsedilen kullanıcıyla ilişkili bilginin şifrelenmemiş bilgi olarak elde edilmesini; görsel sunumun elde edilmesini; bir ortak anahtar kullanarak görsel sunumun görsel görünümü üzerine gömülü şifrelenmiş bilginin şifresinin çözülmesini; görsel sunumdan şifresi çözülmüş bilginin kullanıcıyla ilişkili elde edilen şifrelenmemiş bilgiyle karşılaştırılmasını ve eğer şifresi çözülmüş bilgi bahsedilen kullanıcıyla ilişkili bu şifrelenmemiş bilgiyle aynı ise görsel sunumun söz konusu kullanıcı ile ilişkili olduğunun belirlenmesini içermektedir.

Bu, bir kullanıcının bir sanal dünya ortamında karşılaşılan bir görsel sunumun belirli bir kullanıcıyla ilişkili bir görsel sunum olup olmadığını belirlemesine olanak sağlamaktadır. Bu, eğer karşılaşılan görsel sunum belirli bir kullanıcının bir görsel sunumu ile aynı görse görünüme sahipse ancak karşılığında br canlandırma ise ve aslında bu kullanıcıyla ilişkili değilse faydalıdır.

Bir örnekte yöntem eğer şifresi çözülmüş bilgi kullanıcıyla ilişkili bilgiyle aynı değilse görsel sunumun bahsedilen kullanıcıyla ilişkili olmadığının belirlenmesini içermektedir.

Bir örnekte görsel sunum bir sanal dünya ortamında etkileşim için sağlanan bir avatardır.

Bir örnekte kullanıcı ile ilişkili bilgi bu kullanıcının biyometrik bilgisidir.

Bir örnekte ortak anahtar kullanıcıyla ilişkili bilgidir veya bunu içermektedir.

Bir örnekte kullanıcı ile ilişkili bilgi diğer kullanıcılar için erişilebilir bir veri tabanında depolanmaktadır.

Bir örnekte şifrelenmiş bilgi bir barkodun, bir QR veya matris barkodun, bir renk kodunun ve bir renk modelinin biri veya daha fazlası olarak bir görsel sunumun görsel görünümü üzerine gömülmektedir.

Burada açıklanan bir üçüncü yöne göre aparat sağlanmakta olup, en az bir işlemci; bilgisayar programı talimatlarını içeren en az bir bellek içermektedir; bahsedilen en az bir bellek ve bahsedilen bilgisayar programı talimatları söz konusu en az bir işlemci ile aparatın yukarıda açıklanan yöntemi gerçekleştirmesini sağlamaktadır.

Burada açıklanan bir dördüncü yöne göre bir bilgisayar programı sağlanmakta olup, bilgisayar programı bir veya daha fazla hesaplama cihazında uygulandığı zaman bir veya daha fazla hesaplama cihazının bir özel anahtar kullanarak kullanıcıyla ilişkili bilgiyi şifrelemek; şifrelenmiş bilgiyi şifrelenmiş bilginin başka bir kullanıcı için görünür olacağı şekilde bahsedilen kullanıcıyla ilişkili bir görsel sunumu görsel görünümü üzerine gömmek; söz konusu kullanıcıyla ilişkili bilgiyi şifrelenmemiş bilgi olarak bahsedilen diğer kullanıcı için bulunabilir kılmak ve bahsedilen diğer kullanıcı için bulunabilir şifrelenmiş bilginin şifresini çözmek üzere bir ortak anahtar sağlamak için düzenleneceği bu sayede bahsedilen diğer kullanıcının bu kullanıcıyla ilişkili görsel sunumun görsel görünümü üzerine gömülen bu şifrelenmiş bilginin şifresini çözebileceği ve şifresi çözülmüş bilgiyi diğer kullanıcılar için şifrelenmemiş bilgi olarak bulunabilir kılan bilgiyle karşılaştırabileceği şekilde talimatlar içermektedir.

Burada açıklanan bir beşinci yöne göre bir bilgisayar programı sağlanmakta olup, bilgisayar programı bir veya daha fazla bilgisayar üzerinde uygulandığı zaman bir veya bilgisayar programının kullanıcıyla ilişkili bilgiyi şifrelenmemiş olarak elde etmek; görsel sunumu elde etmek; bir ortak anahtar kullanarak bahsedilen görsel sunumun görsel görünümü üzerine gömülü şifrelenmiş bilginin şifresini çözmek; bu görsel sunumdan şifresi çözülmüş bilgiyi kullanıcıyla ilişkili elde edilen bilgi ile karşılaştırmak ve eğer

bahsedilen şifresi çözülmüş bilgi söz konusu kullanıcıyla ilişkili bu şifrelenmemiş bilgiyle aynı ise bu görsel sunumun bahsedilen kullanıcıya ilişkili olduğunu belirlemek için düzenleneceği şekilde talimatları içermektedir.

Bir örnekte bilgisayar programı, bilgisayar programı bir veya daha fazla hesaplama cihazında uygulandığı zaman bir veya daha fazla hesaplama cihazının eğer şifresi çözülmüş bilgi kullanıcıyla ilişkili bilgiyle aynı değilse görsel sunumun bahsedilen kullanıcıyla ilişkili olduğunu belirlemek için düzenleneceği şekilde talimatları içermektedir.

Bir örnekte görsel sunum bir sanal dünya ortamında etkileşim için sağlanan bir avatardır.

Bir örnekte kullanıcı ile ilişkili bilgi bu kullanıcının biyometrik bilgisidir.

Bir örnekte şifrelenmiş bilgi bir barkodun, bir QR veya matris barkodun, bir renk kodunun ve bir renk modelinin biri veya daha fazlası olarak bir görsel sunumun görsel görünümü üzerine gömülmektedir.

## Şekillerin Kısa Açıklaması

Mevcut patent hakkı bildiriminin anlaşılmasına yardımcı olmak ve uygulamaların nasıl uygulamaya koyulduğunu göstermek için ekli çizimlere örnek yoluyla atıfta bulunulmakta olup, şekillerde:

Şekil 1, bir görsel sunumun üzerine gömülü bir birinci kullanıcının bu birinci kullanıcıyla ilişkili şifrelenmiş bilgisine ilişkin bir örneği şematik olarak göstermektedir.

## Ayrıntılı Açıklama

Bir çevrimiçi çok oyunculu bilgisayar oyunu veya benzerleri gibi sanal dünya ortamında her bir gerçek dünya kullanıcısı özel bir avatarı kontrol etmekte ve/veya bununla karakterize edilmektedir. Bir avatar bir kullanıcının sanal dünya ortamındaki bir görsel temsilidir. Bir kullanıcı avatarın görsel olarak diğer kullanıcılara ait olan avatarlardan ayrılması için görsel görünümünü ihtiyaca göre düzenleyebilmektedir, böylece diğer kullanıcılar bahsedilen kullanıcının avatarını sanal dünya ortamında gördüğü zaman

bahsedilen diğer kullanıcılar bu avatarı söz konusu kullanıcıya ait olduğunu anlayabilmektedir.

Ancak bazı sanal dünya ortamları kasıtsız olarak kullanıcıların kendi avatarların görsel görünümünü başka bir kullanıcının avatarını kişileştirmek veya taklit etmek için modifiye etmesine olanak sağlayabilmektedir. Bu belirli durumlarda özellikle sanal bir dünyadaki bir avatarın belirli bir kullanıcı ile ilişkili olup olmadığını doğrulamak için mekanizma bulunmadığı zaman sorunludur. Eğer kullanıcılar belirli bir avatarın belirli bir kullanıcının olduğundan emin olmazsa o zaman sanal dünya ortamı tarafından sağlanan deneyimin zevk azalmaktadır. Başka bir kullanıcının kişileştirilmesi ayrıca sahtekarlık ve hırsızlık gibi bazı ciddi sorunlara neden olabilmektedir.

Şimdi Şekil 1'e atıfta bulunursak şematik olarak bir birinci kullanıcı (1) gösterilmektedir. Birinci kullanıcı (1) gerçek dünyadadır. Bilgi (2) birinci kullanıcıyla (1) ilişkilidir. Bilgi (2) birinci kullanıcıya (1) ilişkin karakteristiktir ve bahsedilen birinci kullanıcıyı (1) tanımlamak ve bu kullanıcıyı diğer kullanıcılardan ayırt etmek için kullanılabilmektedir. Bu örnekte bu bilgi (2) birinci kullanıcının (1) biyometrik bilgisidir. Bu örneğin bir kullanıcının parmak izi veya avuç içi izi, bir kullanıcının yüzünün özelliklerinin bir haritası, bu kullanıcının retinasının bir taraması veya benzerleri gibi kendine özgü bir biyometrik tanımlayıcı olabilmektedir.

Birinci kullanıcı (1) bir görsel sunuma (3) sahiptir. Birinci kullanıcının (1) görsel sunumu (3) bu birinci kullanıcıyı (1) bir çevrimiçi oyun gibi bir sanal dünya ortamında temsil etmektedir. Bu örnekte görsel sunum (3) bir sanal karakter örn, bir avatardır. Görsel sunumun (3) görsel görünümü (başka bir deyişle, sanal dünya ortamında diğer kullanıcılara görünebilir olan görsel sunumun (3) yüzeyi) değiştirilebilmekte ve birinci kullanıcı (1) tarafından isteğe göre uyarlanabilmektedir.

Şimdi bir ikinci kullanıcının (4) görsel sunumun (3) birinci kullanıcının (1) bir sunumu olduğunu ve başka bir kullanıcının bir sunumu olmadığını doğrulamasına olanak sağlamaya ilişkin bir yöntem açıklanacaktır.

Birinci kullanıcı (2) ile ilişkili bilgi (2) bir kamusal/özel anahtar çiftinin bir özel anahtarı kullanılarak şifrelenmektedir. Kimlik doğrulama ve şifrelemeye yönelik kamusal/özel

anahtar çiftlerinin kullanımı kendi içinde iyi bilinmektedir ve burada detaylı şekilde açıklanmayacaktır.

Şifrelenmiş bilgi daha sonra birinci kullanıcının (1) görsel sunumunun (3) görsel görünümü (başka bir deyişle, dış yüzeyi) üzerine gömülmekte veya buraya kaynaştırılmaktadır. Gömüşü şifrelenmiş bilgi (5) birinci kullanıcının (1) görsel sunumunun (3) mevcut olduğu bir sanal dünya ortamındaki diğer kullanıcılara (örneğin ikinci kullanıcı (4)) görünür olacağı bir formda gömülmektedir. Bu örnekte şifrelenmiş bilgi birinci kullanıcının (1) görsel sunumunun (3) görsel görünümü üzerine bir barkod olarak gömülmektedir. Başka bir örnekte şifrelenmiş bilgi bir QR veya matris barkod, bir renk kodu veya bir renk modeli gibi farklı bir tip görsel tanımlayıcı olarak gömülmektedir. Gömülü şifrelenmiş bilgi (5) diğer kullanıcılara bu diğer kullanıcıların bir işleme cihazının örneğin bir kamera ve/veya bazı işleme cihazları kullanarak gömüşü şifrelenmiş bilgiyi (5) “görebileceği” ve okuyabileceği bir formda gömülmektedir.

Birinci kullanıcıyla (1) ilişkili bilgi (2) ayrıca diğer kullanıcılar için bulunabilir kılınmakta olup, burada ikinci kullanıcıyı (4) içermektedir. Bilgi (2) şifrelenmemiş bilgi olarak bulunabilir kılınmaktadır böylece diğer kullanıcılar (bunların işleme cihazları) vasıtasıyla okunabilmektedir. Bu örnekte birinci kullanıcı (1) ile ilişkili bilgi (2) diğer kullanıcılar için erişilebilir bir veri tabanında (6) depolanmaktadır. Veri tabanında (6) depolanan birinci kullanıcıyla (1) ilişkili bilgi (2) örneğin herhangi bir kullanıcı için ortak olarak bulunabilir veya sadece bir şifre, giriş ayrıntıları, vs. gibi uygun referansların girişi üzerine kullanıcılar için bulunabilir olabilmektedir. Başka bir örnekte bilgi (2) birinci kullanıcı (1) tarafından sadece bir veya daha fazla spesifik ikinci kullanıcıya (4) (örneğin bahsedilen birinci kullanıcının (1) güvenilir arkadaşları veya eş dostları olabilmektedir) iletilebilmektedir. Başka bir örnekte bilgi (2) eşler arası ağ oluşturma vasıtasıyla transfer edilebilmektedir.

Birinci kullanıcıyla ilişkili şifrelenmiş bilginin şifresini çözmeye yönelik kamusal/özel anahtar çiftinin ortak anahtarı ayrıca ikinci kullanıcı (4) için veya birden çok kullanıcı için bulunabilir kılınmaktadır böylece bunlar gömülü şifrelenmiş bilginin (5) şifresini çözebilmektedir. Bir örnekte ortak anahtar sadece ikinci kullanıcı (4) tarafından talep edildiği zaman bahsedilen ikinci kullanıcı (4) için erişilebilir kılınabilmektedir. Alternatif olarak yukarıda tartışılan bilgiye (2) benzer şekilde ortak anahtar diğer kullanıcılar için bulunabilir bir veri tabanında (6) depolanabilmektedir. Veri tabanında (6) depolanan ortak

anahtar örneğin herhangi bir kullanıcı için ortak olarak bulunabilir veya sadece bir şifre, giriş ayrıntıları, vs. gibi uygun referansların girişi üzerine kullanıcılar için bulunabilir olabilmektedir. Başka bir örnekte ortak anahtar birinci kullanıcı (1) tarafından sadece bir veya daha fazla spesifik ikinci kullanıcıya (4) (örneğin yine bahsedilen birinci kullanıcının (1) güvenilir arkadaşları veya eş dostları olabilmektedir) iletilebilmektedir. Başka bir örnekte ortak anahtar bilginin (2) kendisi olabilmektedir.

Bu ikinci kullanıcının (4) bir sanal dünya ortamında karşılaşılan bir görsel sunumunun birinci kullanıcının (1) görsel sunumu (3) olup olmadığını belirlemesini sağlamaktadır. Bu doğrulamaya ilişkin başka bir örnek şimdi açıklanacaktır.

Birinci kullanıcıyla (1) ilişkili bilgi (2) ikinci kullanıcı (4) (kullanıcının bir bilgisayarı) tarafından elde edilmektedir. Bu örnekte bilginin (2) şifrelenmemiş bir formda depolandığı bir veri tabanına erişmek için giriş detayları önceden örneğin birinci kullanıcı (1) tarafından veya örneğin kullanıcıların sunumlarının bulunduğu ortamın çalıştırılmasından sorumlu olabilen bazı yöneticiler tarafından ikinci kullanıcı (4) için bulunabilir kılınmıştır.

Karşılaşılan görsel sunum sana dünya ortamından elde edilmektedir. Buna bir görüntüleme ekranında sanal dünyayı görüntüleyen ayrı bir kamera kullanılarak erişilebilmektedir. Alternatif olarak veya ilaveten karşılaşılan görsel sunum ikinci kullanıcının (4) sanal dünyasına ilişkin görüntülerin lokal olarak oluşturulmasına dahil olan bir video işleme cihazından veya bu cihaz kullanılarak elde edilebilmektedir. Görsel sunum kendi görsel görünümü üzerine gömülü şifrelenmiş bilgiyi içermektedir. Gömülü şifrelenmiş bilgi (5) görsel sunumun bu örnekte (iddiaya göre) birinci kullanıcı (1) olan sahibini doğrulamak için kullanılabilmektedir.

Birinci kullanıcı (1) tarafından ikinci kullanıcı (4) için bulunabilir kılınmış olan ortak anahtar ayrıca elde edilebilmektedir. Elde edilen ortak anahtar görsel sunumun yüzeyinden okunduktan sonra gömüşü şifrelenmiş bilginin (5) şifresini çözmek için kullanılmaktadır.

Birinci kullanıcının (1) görsel sunumundan veya avatarından elde edilen şifresi çözülmüş bilgi daha sonra bahsedilen birinci kullanıcı (1) tarafından şifrelenmemiş formda bulunabilir kılınmış bilgiyle (2) karşılaştırılmaktadır. Eğer şifresi çözülmüş bilginin birinci kullanıcı (1) tarafından bulunabilir kılınmış bilginin (2) şifrelenmemiş formuyla aynı olduğu

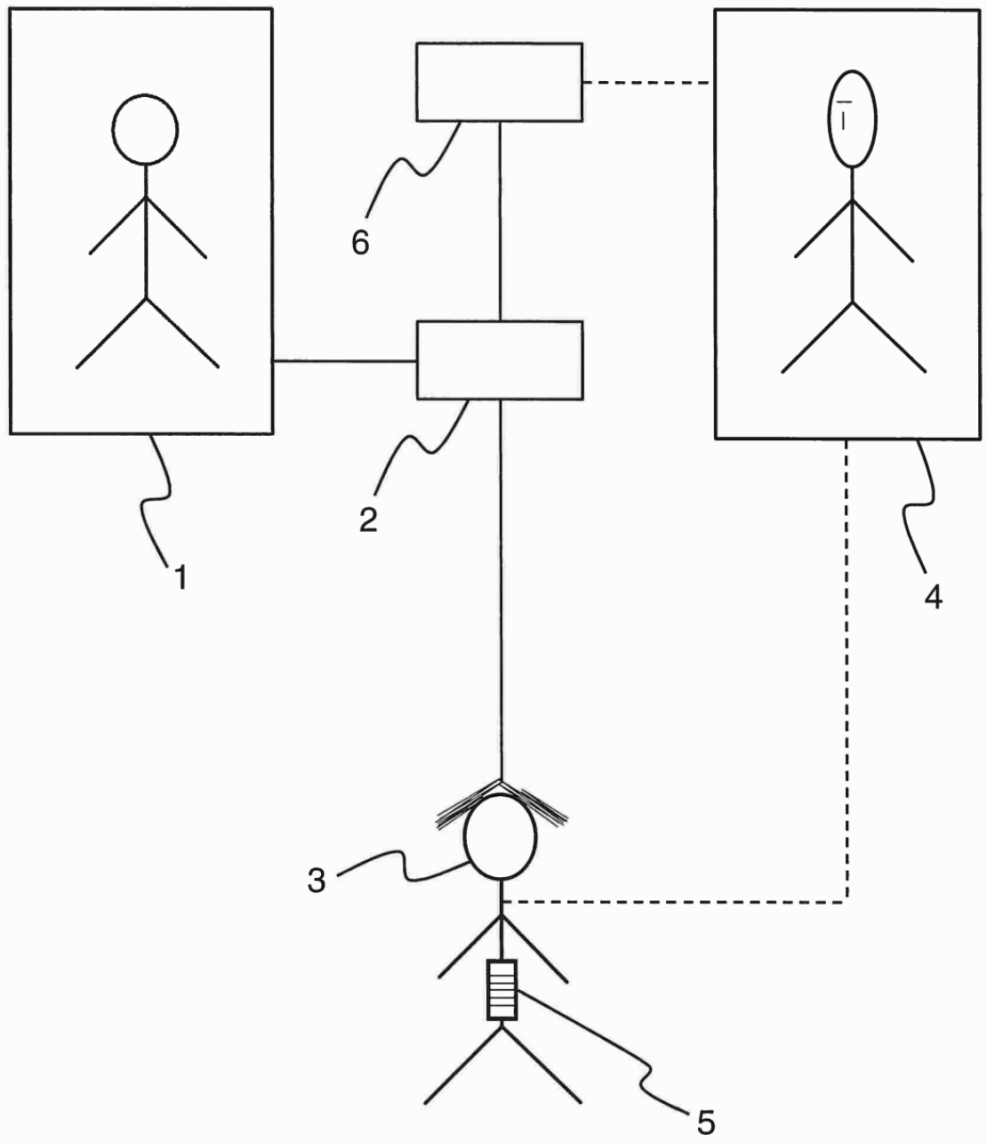
bulunursa o zaman şifresi çözülmüş bilginin bahsedilen birinci kullanıcıdan (1) kaynaklandığı ve dolayısıyla ikinci kullanıcı (4) tarafından karşılaşılan görse sunumun bahsedilen birinci kullanıcının (1) görsel sunumu (3) olduğu belirlenebilmektedir. Eğer şifresi çözülmüş bilginin birinci kullanıcı (1) tarafından bulunabilir kılınmış bilginin (2) şifrelenmemiş formuyla aynı olmadığı bulunursa o zaman şifresi çözülmüş bilginin bahsedilen birinci kullanıcıdan (1) kaynaklanmadığı ve dolayısıyla ikinci kullanıcı (4) tarafından karşılaşılan görse sunumun bahsedilen birinci kullanıcının (1) görsel sunumu olmadığı belirlenebilmektedir.

Bu düzenlemenin bir avantajı bir sanal dünyada karşılaşılan bir görsel sunumun gerçekten birinci kullanıcı ile ilişkili olan (ve tipik olarak bunun tarafından kontrol edilen) bir görsel sunum olup olmadığını belirlemek için birinci kullanıcının ikinci kullanıcı (ve diğer kullanıcılar) için bir yol sağlayabilmesidir. Bu özellikle ikinci kullanıcının (ve diğer kullanıcıların) birinci kullanıcının bir özgün görsel sunumu ve bahsedilen birinci kullanıcıyı kişileştirmek için kullanılmakta olan bir görsel sunum arasında ayrım yapmasını sağlamada yardımcı olmaktadır. Bu, ikinci kullanıcı sanal dünyada gezinirken ve bahsedilen ikinci kullanıcı tarafından spesifik hareketler alınmasını gerektirmeden arka planda çalışan işlemler tarafından hızlıca ve sorunsuz bir şekilde gerçekleştirilebilmektedir.

Her ne kadar ekli şekillere atıfta bulunarak burada açıklanan uygulamaların bazı yönleri işleme sistemleri veya işlemcilerde gerçekleştirilen bilgisayar işlemleri içerse dahi buluş ayrıca bilgisayar programlarına, özellikle buluşu uygulamaya koymak için uyarlanan, bir taşıyıcı üzerindeki veya içindeki bilgisayar programlarına genişletilmektedir. Program kısmen derlenmiş form veya buluşa göre işlemlerin uygulanmasında kullanım için uygun herhangi başka bir geçici olmayan form gibi geçici olmayan kaynak kodu, nesne kodu, bir kod ara kaynağı ve nesne kodu formunda olabilmektedir. Taşıyıcı programı taşıyabilen herhangi bir entite veya cihaz olabilmektedir. Örneğin taşıyıcı bir katı-hal sürücüsü (SSD) veya başka yarı iletken tabanlı RAM gibi bir depolama ortamı; bir ROM örneğin bir CD ROM veya bir yarı iletken ROM; bir manyetik kayıt ortamı örneğin bir disket veya hard disk; genel olarak optik bellek cihazları; vs. içerebilmektedir.

Burada açıklanan örnekler buluşun uygulamalarına ilişkin açıklayıcı örnekler olarak anlaşılmalıdır. Diğer uygulamalar ve örnekler tasarlanmaktadır. Herhangi bir örnekle

veya uygulamayla ilişkili açıklanan herhangi br özellik tek başına veya diğer özelliklerle kombinasyon halinde kullanılabilmektedir. Ek olarak herhangi bir örnek veya uygulama ile ilişkili şekilde açıklanan herhangi bir özellik ayrıca örneklerin veya uygulamaların herhangi birinin bir veya daha fazla özelliği veya örneklerin veya uygulamaların herhangi birinin herhangi bir kombinasyonu ile kombinasyon halinde kullanılabilmektedir. Bunun ötesinde burada açıklanmayan eşdeğerler ve modifikasyonlar da ayrıca istemlerde açıklanan buluşun kapsamı içinde kullanılabilmektedir.




**Şekil 1**